

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006215

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-196531
Filing date: 02 July 2004 (02.07.2004)

Date of receipt at the International Bureau: 09 June 2005 (09.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2005/006215

日 本 国 特 許 庁
JAPAN PATENT OFFICE

24.03.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 7 月 2 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 1 9 6 5 3 1

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号
The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

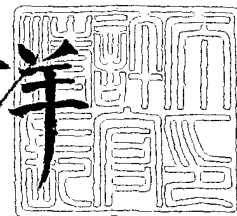
J P 2 0 0 4 - 1 9 6 5 3 1

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 5 月 2 6 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



出証番号 出証特 2 0 0 5 - 3 0 4 5 6 4

【書類名】 特許願
【整理番号】 2048160232
【提出日】 平成16年 7月 2日
【あて先】 特許庁長官殿
【国際特許分類】 G09L 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 野仲 真佐男
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 布田 裕一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 横田 薫
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 宮崎 雅也
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 山本 雅哉
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 村瀬 薫
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1

【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9809938

【書類名】特許請求の範囲**【請求項 1】**

不正コンテンツを検知する不正コンテンツ検知システムであって、

前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、

前記配布センタは、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、

一以上の前記検証データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、

前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、

前記実行装置は、

前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、

前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記一以上の第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、

を備えることを特徴とする不正コンテンツ検知システム。

【請求項 2】

不正コンテンツを検知する不正コンテンツ検知システムであって、

前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、

前記配布センタは、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含む

データに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、

一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、

前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、

前記実行装置は、

前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、

前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、

を備えることを特徴とする不正コンテンツ検知システム。

【請求項3】

コンテンツを実行、もしくは再生する実行装置であって、

前記実行装置は、

前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記第一属性値の数に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、

を備えることを特徴とする実行装置。

【請求項4】

コンテンツを実行、もしくは再生する実行装置であって、

前記実行装置は、

前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、

前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、

前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、

を備えることを特徴とする実行装置。

【請求項 5】

前記取得部は、可搬媒体からデータを取得すること、

を特徴とする、請求項 3 または請求項 4 に記載の実行装置。

【請求項 6】

前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、

を特徴とする、請求項 3 または請求項 4 に記載の実行装置。

【請求項 7】

前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、

を特徴とする、請求項 3 から請求項 6 のいずれか 1 項に記載の実行装置。

【請求項 8】

前記実行装置は、さらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、

前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、

前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、

を特徴とする、請求項 3 から請求項 7 のいずれか 1 項に記載の実行装置。

【請求項 9】

前記実行装置は、さらに、

前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、

前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、

を特徴とする、請求項 8 に記載の実行装置。

【請求項 10】

前記実行装置は、さらに、

デバイス鍵を保持するデバイス鍵格納部と、

前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、

前記取得部はさらに、前記暗号化鍵束を受信すること、

を特徴とする、請求項 8 または請求項 9 に記載の実行装置。

【請求項 11】

前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、

を特徴とする、請求項 3 から請求項 10 のいずれか 1 項に記載の実行装置。

【請求項 12】

前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること

、
を特徴とする、請求項 3 から請求項 1 0 のいずれか 1 項に記載の実行装置。

【請求項 1 3】

前記検証情報は、デジタル署名方式の検証鍵であること、
を特徴とする、請求項 3 から請求項 1 2 のいずれか 1 項に記載の実行装置。

【請求項 1 4】

前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、

前記取得部はさらに、前記検証情報識別子を受信し、

前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、

を特徴とする、請求項 3 から請求項 1 3 のいずれか 1 項に記載の実行装置。

【請求項 1 5】

前記取得部はさらに、前記検証情報を受信すること、

を特徴とする、請求項 3 から請求項 1 4 のいずれか 1 項に記載の実行装置。

【請求項 1 6】

前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、

前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、

を特徴とする、請求項 1 4 から請求項 1 5 のいずれか 1 項に記載の実行装置。

【請求項 1 7】

前記実行装置は、さらに、

前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、
前記検証情報格納部に保持する第二取得部を備えること、

を特徴とする、請求項 1 6 に記載の実行装置。

【請求項 1 8】

前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、

を特徴とする、請求項 1 7 に記載の実行装置。

【請求項 1 9】

前記第二取得部と前記取得部は等しいこと、

を特徴とする、請求項 1 7 または請求項 1 8 に記載の実行装置。

【請求項 2 0】

前記コンテンツは、前記実行装置で実行可能なプログラムであり、

前記実行部は、前記プログラムを実行すること、

を特徴とする請求項 3 から請求項 1 9 のいずれか 1 項に記載の実行装置。

【請求項 2 1】

コンテンツを配布する配布センタであって、

前記配布センタは、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、
対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含む

データに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、

一以上の前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、

前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、

を備えることを特徴とする配布センタ。

【請求項 22】

コンテンツを配布する配布センタであって、

前記配布センタは、

前記コンテンツを入力する入力部と、

認証情報生成情報を保持する認証情報生成情報格納部と、

前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、

一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、

前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、

を備えることを特徴とする配布センタ。

【請求項 23】

前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、

を特徴とする、請求項 21 または請求項 22 に記載の配布センタ。

【請求項 24】

前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、

を特徴とする、請求項 21 から請求項 23 のいずれか 1 項に記載の配布センタ。

【請求項 25】

前記配布センタはさらに、

コンテンツ鍵を保持するコンテンツ鍵格納部と、

前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、

前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、

を特徴とする、請求項 21 から請求項 24 のいずれか 1 項に記載の配布センタ。

【請求項 26】

前記配布センタはさらに

一以上のデバイス鍵を保持する実行装置情報格納部と、

前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、

前記配布部はさらに、前記暗号化鍵束を配布すること、

を特徴とする、請求項 25 に記載の配布センタ。

【請求項 27】

前記配布センタはさらに

前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、

前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、
を特徴とする、請求項 25 または請求項 26 に記載の配布センタ。

【請求項 28】

前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、
を特徴とする、請求項 21 から請求項 27 のいずれか 1 項に記載の配布センタ。

【請求項 29】

前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること
、
を特徴とする、請求項 21 から請求項 27 のいずれか 1 項に記載の配布センタ。

【請求項 30】

前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする、請求項 21 から請求項 29 のいずれか 1 項に記載の配布センタ。

【請求項 31】

前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布
すること、
を特徴とする、請求項 21 から請求項 30 のいずれか 1 項に記載の配布センタ。

【請求項 32】

前記配布センタはさらに、
前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテン
ツ位置情報生成部を備えること、
を特徴とする、請求項 21 から請求項 31 のいずれか 1 項に記載の配布センタ。

【請求項 33】

前記コンテンツ位置情報生成部はさらに
外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、
を特徴とする、請求項 32 に記載の配布センタ。

【請求項 34】

前記コンテンツ位置情報生成部はさらに、
ランダムに前記コンテンツ位置情報を生成すること、
を特徴とする、請求項 32 に記載の配布センタ。

【書類名】 明細書

【発明の名称】 不正コンテンツ検知システム

【技術分野】

【0001】

本発明は不正なコンテンツを検知する技術に関するものである。

【背景技術】

【0002】

近年、デジタルコンテンツの普及に伴い、著作権を保持する者以外がデジタルコンテンツを不正に販売する、いわゆる違法コンテンツの不正配布が社会問題となってきた。このコンテンツ不正配布の一つのケースとして、映画館等で上映される映画コンテンツを、著作権を保持しない第三者がデジタルビデオカメラ等で盗撮し、その盗撮した動画コンテンツを光ディスクに記録し販売するというものが挙げられる。また別のケースとして、正規に販売されている片面2層DVD-ROMディスク（最大8.5ギガバイト）に記録されているDVD-VIDEO形式の映画コンテンツの画質を変換処理して4.7ギガバイト以下に収まるようにして、片面1層DVD-Rディスク（最大4.7ギガバイト）に記録して販売するものも挙げられる。

【0003】

上記のようなコンテンツ不正利用を防ぐ方法の従来技術としては、特許文献1に記載されている不正コンテンツ検知システムが知られている。この従来技術は、可搬媒体の中に、コンテンツデータの他に、複数の部分コンテンツデータに対応するハッシュ値と、複数のハッシュ値を結合したデータに対する著作権者のデジタル署名と、を記録しておく。そして、実行装置では、可搬媒体の中のコンテンツを再生する前と、コンテンツを再生している途中に、記録されたコンテンツデータが正規の著作権者によって記録されたものか、デジタル署名及びハッシュ値を用いて検証を行う。そして、検証が失敗したら、コンテンツの再生を停止するものである。こうすることにより、正規の著作権者でない第三者が映画館等において盗撮したコンテンツを可搬媒体に記録して販売したとしても、その可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置はコンテンツを正しく再生しない。これにより、不正なコンテンツの配布防止につながる。

【0004】

ここでは、従来技術の詳細の一例について図33を用いて説明する。前提として、正規の著作権者はデジタル署名を作成するための署名生成鍵を有しており、実行装置はその署名生成鍵に対応する署名検証鍵を有しているとする。

【0005】

初めに、正規の著作権者が、コンテンツデータと、複数の部分コンテンツデータに対応するハッシュ値と、複数のハッシュ値を結合したデータに対するデジタル署名と、を記録した可搬媒体を生成する場合の動作について説明する。まず、デジタルコンテンツを c 個（ c は2以上の自然数）のコンテンツブロック（図33のコンテンツブロックBLK1・・・・BLK c に対応）に分割する。そして、一方向性関数を用いてコンテンツブロックBLK1のハッシュ値HASH1を計算する。コンテンツブロックBLK2以降も同様にハッシュ値を計算し、それぞれのコンテンツブロックBLK2、・・・、BLK c に対応するハッシュ値HASH2、・・・、HASH c を求める。そして、 c 個のハッシュ値HASH1、・・・、HASH c を連結させたものをヘッダ情報HEADとする。その後、正規の著作権者の署名生成鍵を用いて、そのヘッダ情報HEADのデジタル署名を生成し、そのデジタル署名とヘッダ情報とコンテンツを可搬媒体に記録し、実行装置へ提供する。

【0006】

続いて、実行装置が、提供された可搬媒体内のコンテンツを再生する場合の動作について説明する。まず、署名検証鍵を用いてデジタル署名が正規の著作権者によるヘッダ情報のデジタル署名であるかを検証する。そこで、もし正規のデジタル署名であることが確認されれば、コンテンツの再生を開始する。その後、実行装置はコンテンツを再生しながら

、再生しているコンテンツブロックのハッシュ値を計算し続ける。そして、次のコンテンツブロックに再生位置が移動する際に、計算したハッシュ値がヘッダ情報のハッシュ値と一致するかを確認し、もし一致しなかった場合、コンテンツの再生を停止する。

【0007】

このような従来技術により、何らかの理由によりコンテンツが盗み出され、そのコンテンツを可搬媒体に記録して販売しようとしても、可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置ではそのコンテンツを再生開始しないか、もしくは、途中で再生が停止する。これにより、不正なコンテンツ流通に対する対策が可能となる。

【特許文献1】米国特許第6480961号明細書

【特許文献2】特開2002-281013号公報

【非特許文献1】「情報セキュリティ」宮地充子・菊池浩明編著 情報処理学会編集

【非特許文献2】「THE ART OF COMPUTER PROGRAMMING Vol. 2 ~ SEMINUMERICAL ALGORITHMS」DONALD E. KNUTH 著、ISBN 0-201-03822-6

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、前記従来技術では、実行装置がコンテンツを再生している間、継続してコンテンツブロックのハッシュ値を計算し続けなければならないので、コンテンツ再生中の実行装置の処理負荷が高いという課題を有していた。例えば、一般に、コンテンツは暗号化されて配布されるため、再生する直前にコンテンツを復号化する必要がある。このような場合、コンテンツを復号化すると同時に、復号化したコンテンツのハッシュ値を計算しなければならないという課題があった。

【0009】

本発明は、前記従来技術の課題を解決するもので、コンテンツ再生中の実行装置の処理負荷を軽減させた不正コンテンツ検知システムを提供することを目的とする。

【課題を解決するための手段】

【0010】

上記課題を解決するために、請求項1における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選

択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記一以上の第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0011】

請求項2における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0012】

請求項3における発明は、コンテンツを実行、もしくは再生する実行装置であって、前記実行装置は、前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記第一属性値の数に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属

性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0013】

請求項4における発明は、コンテンツを実行、もしくは再生する実行装置であって、前記実行装置は、前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【0014】

請求項5における発明は、請求項3または請求項4に記載の実行装置であって、前記取得部は、可搬媒体からデータを取得すること、を特徴とする。

【0015】

請求項6における発明は、請求項3または請求項4に記載の実行装置であって、前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、を特徴とする。

【0016】

請求項7における発明は、請求項3から請求項6のいずれか1項に記載の実行装置であって、前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、を特徴とする。

【0017】

請求項8における発明は、請求項3から請求項7のいずれか1項に記載の実行装置であって、前記実行装置は、さらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、を特徴とする。

【0018】

請求項9における発明は、請求項8に記載の実行装置であって、前記実行装置は、さらに、前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、を特徴とする。

【0019】

請求項10における発明は、請求項8または請求項9に記載の実行装置であって、前記実行装置は、さらに、デバイス鍵を保持するデバイス鍵格納部と、前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、前記取得部はさらに、前記暗号化鍵束を受信すること、を特徴とする。

【0020】

請求項 11 における発明は、請求項 3 から請求項 10 のいずれか 1 項に記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。

【0021】

請求項 12 における発明は、請求項 3 から請求項 10 のいずれかに記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。

【0022】

請求項 13 における発明は、請求項 3 から請求項 12 のいずれか 1 項に記載の実行装置であって、前記検証情報は、デジタル署名方式の検証鍵であること、を特徴とする。

【0023】

請求項 14 における発明は、請求項 3 から請求項 13 のいずれか 1 項に記載の実行装置であって、前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、前記取得部はさらに、前記検証情報識別子を受信し、前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【0024】

請求項 15 における発明は、請求項 3 から請求項 14 のいずれか 1 項に記載の実行装置であって、前記取得部はさらに、前記検証情報を受信すること、を特徴とする。

【0025】

請求項 16 における発明は、請求項 14 または請求項 15 に記載の実行装置であって、前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【0026】

請求項 17 における発明は、請求項 16 に記載の実行装置であって、前記実行装置は、さらに、前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、を特徴とする。

【0027】

請求項 18 における発明は、請求項 17 に記載の実行装置であって、前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、を特徴とする。

【0028】

請求項 19 における発明は、請求項 17 または請求項 18 に記載の実行装置であって、前記第二取得部と前記取得部は等しいこと、を特徴とする。

【0029】

請求項 20 における発明は、請求項 3 から請求項 19 のいずれか 1 項に記載の実行装置であって、前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。

【0030】

請求項 21 における発明は、コンテンツを配布する配布センタであって、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性

値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、を備えることを特徴とする。

【0031】

請求項 22 における発明は、コンテンツを配布する配布センタであって、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、を備えることを特徴とする。

【0032】

請求項 23 における発明は、請求項 21 または請求項 22 に記載の配布センタであって、前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、を特徴とする。

【0033】

請求項 24 における発明は、請求項 21 から請求項 23 のいずれか 1 項に記載の配布センタであって、前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、を特徴とする。

【0034】

請求項 25 における発明は、請求項 21 から請求項 24 のいずれか 1 項に記載の配布センタであって、前記配布センタはさらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、前記配布部は、前記コンテンツの代わりに前記暗号化コンテンツを配布すること、を特徴とする。

【0035】

請求項 26 における発明は、請求項 25 に記載の配布センタであって、前記配布センタはさらに一以上のデバイス鍵を保持する実行装置情報格納部と、前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、前記配布部はさらに、前記暗号化鍵束を配布すること、を特徴とする。

【0036】

請求項 27 における発明は、請求項 25 または請求項 26 のいずれか 1 項に記載の配布センタであって、前記配布センタはさらに前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、を特徴とする。

【0037】

請求項 28 における発明は、請求項 21 から請求項 27 のいずれか 1 項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。

【0038】

請求項29における発明は、請求項21から請求項27のいずれか1項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。

【0039】

請求項30における発明は、請求項21から請求項29のいずれか1項に記載の配布センタであって、前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、を特徴とする。

【0040】

請求項31における発明は、請求項21から請求項30のいずれか1項に記載の配布センタであって、前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、を特徴とする。

【0041】

請求項32における発明は、請求項21から請求項31のいずれか1項に記載の配布センタであって、前記配布センタはさらに、前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、を特徴とする。

【0042】

請求項33における発明は、請求項32に記載の配布センタであって、前記コンテンツ位置情報生成部はさらに外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、を特徴とする。

【0043】

請求項34における発明は、請求項32に記載の配布センタであって、前記コンテンツ位置情報生成部はさらに、ランダムに前記コンテンツ位置情報を生成すること、を特徴とする。

【発明の効果】**【0044】**

本発明の不正コンテンツ検知システムによれば、コンテンツを実行開始、もしくは再生開始する前にのみ、コンテンツが正規の著作権者により配布されたコンテンツ（正規コンテンツ）なのか、正規の著作権者以外により配布されたコンテンツ（不正コンテンツ）なのかを検証し、コンテンツの実行中、再生中にはその検証を行わないようにした。そうすることにより、不正コンテンツの実行、再生を制限（開始不許可など）することが出来るようになるとともに、従来技術に比べ、コンテンツ実行中、再生中の実行装置の処理負荷を軽減出来るようになった。

【0045】

また、本発明の不正コンテンツ検知システムでは、さらに、実行装置がコンテンツを実行、再生開始する場合に、暗号化コンテンツの一部分の属性値（ハッシュ値）を検証するようにした。これにより、従来技術のように、暗号化コンテンツを一度復号化して属性値を検証する場合に比べ、処理時間を短縮することが出来た。

【0046】

また、検証時に、実行装置が同じコンテンツを実行、再生する場合にも、コンテンツの中の毎回異なる一部分の属性値（ハッシュ値）を検証するようにした。これにより、不正者は、次にコンテンツのどの一部分が検証されるのか予測出来ないようになった。

【0047】

この結果、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを実行、再生する場合でも、ある確率（実行装置が不正な部分コンテンツに入れ替えた部分の属性値を検証する場合）で実行、再生の制限（再生不許可など）が出来るようになる。つまり、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを、毎回必ず実行、再生をさせることは出来なく出来る。このことにより、コンテンツの中の全部もしくは一部分を、不正なコンテンツに差し替えられるような攻撃を防ぐことが出来、抑止力となる。

【0048】

これは、コンテンツデータとともに、そのコンテンツデータ全体に対する属性値（ハッシュ値）1つと、その属性値（ハッシュ値）に対するデジタル署名と、を記録した可搬媒体を配布する自明な方式に比べても優位性を持つ。何故なら、自明な方式の場合コンテンツデータ全体に対する属性値（ハッシュ値）を計算しなくてはならないため、コンテンツの実行、再生開始前の処理に時間がかかっていた。しかし、本発明の不正コンテンツ検知システムによれば、コンテンツの実行、再生開始前には、毎回異なるコンテンツの一部分の属性値（ハッシュ値）だけを計算すれば良いので、自明な方式に比べ、処理時間を短縮することが出来る。

【発明を実施するための最良の形態】

【0049】

以下本発明の実施の形態について、図面を参照しながら説明する。

【0050】

（実施の形態1）

図1は、本発明の実施の形態1における不正コンテンツ検知システムの構成図である。図1において、配布センタ10は外部からコンテンツCNTを受け取り、後述する実行装置12がコンテンツCNTを実行するために必要となる情報を後述する可搬媒体11に記録するものであり、可搬媒体11は実行装置12がコンテンツCNTを実行するために必要となる情報が記録されているものであり、複数の実行装置12は可搬媒体11に記録されている情報を用いて、コンテンツCNTを実行するものである。

【0051】

不正コンテンツ検知システム1は、配布センタ10（正規のコンテンツ提供者、著作権者、正規の光ディスクプレス業者など）が、DVD（Digital Versatile Disc）等の可搬媒体11の配布手段によって、暗号化されたコンテンツCNTである暗号化コンテンツENCNTと、暗号化コンテンツENCNTを基に生成されるヘッダ情報HEADと、ヘッダ情報HEADに含まれる第二ハッシュテーブルHASH TBL2の正当性を示す情報である認証情報AUTHを、各実行装置12へ配布する。各実行装置12は、暗号化コンテンツENCNTを基にヘッダ情報HEADの中の一部の情報を入れ替えて入替第二ハッシュテーブルREPHASH TBL2を作成し、認証情報AUTHが配布センタ10による入替第二ハッシュテーブルREPHASH TBL2の正規の認証情報であることを確認し、コンテンツCNTを実行開始する。

【0052】

以上が、本実施の形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施の形態である不正コンテンツ検知システム1の詳細について説明を行う。

【0053】

＜不正コンテンツ検知システム1の構成＞

不正コンテンツ検知システム1は、図1に示すように、配布センタ10と、可搬媒体11と、s個の実行装置12（sは1以上の自然数）から構成される。

【0054】

以下に、これらの構成要素について、詳細に説明する。まず、配布センタ10の構成と動作について述べ、続いて可搬媒体11の構成について述べ、最後に実行装置12の構成と動作について述べる。

【0055】

＜配布センタ10の構成＞

配布センタ10は、図2に示すように、入力部101、コンテンツ鍵生成部102、実行装置情報格納部103、暗号化鍵束生成部104、暗号化部105、ヘッダ情報生成部106、認証情報生成情報格納部107、認証情報生成部108、配布部109から構成される。

【0056】

（1）入力部101

入力部101は、外部からコンテンツCNTを入力出来るものである。入力部101は、例えば、可搬媒体であるDVD-ROM等からコンテンツCNTを読み取る機能を有する。外部から入力されるコンテンツCNTは、実行装置12で実行可能なフォーマット形式であって、例えば、MPEG (Moving Picture Experts Group) 2フォーマット形式による動画データやMP3フォーマットによる音声データなどである。外部からコンテンツCNTが入力された場合、コンテンツ鍵生成要求REQをコンテンツ鍵生成部102へ出力し、コンテンツCNTを暗号化部105へ出力する。

【0057】

(2) コンテンツ鍵生成部102

コンテンツ鍵生成部102は、入力部101からコンテンツ鍵生成要求REQが入力された場合、コンテンツ鍵CKを生成する。コンテンツ鍵CKを生成する方法としては、例えば、乱数を用いて128ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部102が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献2が詳しい。そして、コンテンツ鍵CKを暗号化鍵束生成部104及び暗号化部105へ出力する。なお、コンテンツ鍵CKはコンテンツCNTを暗号化、復号化するための鍵であり、暗号化部105及び実行装置12の実行部126で使用される。

【0058】

(3) 実行装置情報格納部103

実行装置情報格納部103は、複数の実行装置12に与えられる鍵情報を保持するものである。図3は、実行装置情報格納部103の一例を示しており、装置識別子AID1に対応付けられたデバイス鍵DK1と、装置識別子AID2に対応付けられたデバイス鍵DK2と、・・・、装置識別子AIDsに対応付けられたデバイス鍵DKsを保持している状態を示している。ここで、装置識別子AID1、AID2、・・・、AIDsのそれぞれは、複数の実行装置12のいずれかに対応付けられており、デバイス鍵DK1、DK2、・・・、DKsのそれぞれは、対応する実行装置12のデバイス鍵格納部122に格納されている鍵である。なお、デバイス鍵DK1、DK2、・・・、DKsのそれぞれはコンテンツ鍵CKを暗号化、復号化するための鍵であり、暗号化鍵束生成部104及びコンテンツ鍵取得部123で用いられる。例えば、装置識別子AID1、AID2、・・・、AIDsは、それぞれ異なる自然数1、2、・・・、nであり、デバイス鍵DK1、DK2、・・・、DKsは、例えば、それぞれ異なる128ビット鍵データである。

【0059】

(4) 暗号化鍵束生成部104

暗号化鍵束生成部104は、コンテンツ鍵生成部102からコンテンツ鍵CKが入力された場合、実行装置情報格納部103にアクセスして複数の実行装置12が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵CKとを基に、暗号化鍵束KBを生成する。暗号化鍵束KBは、各実行装置12がその暗号化鍵束KBと自身の保持する鍵を用いてコンテンツ鍵CKが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置12はそれぞれ、AID1からAIDsのいずれかの装置識別子と対応するデバイス鍵(DK1、・・・、DKsのいずれか)を保持しており、実行装置情報格納部103には、図3のように、実行装置12が保持する装置識別子(AID1、・・・、AIDs)と対応するデバイス鍵(DK1、・・・、DKs)の組が全て格納されているとする。そのような場合、暗号化鍵束KBは例えば以下のように生成される。実行装置情報格納部103から装置識別子AID1と対応するデバイス鍵DK1を取得する。そして、デバイス鍵DK1を基にコンテンツ鍵CKを暗号化し、暗号化コンテンツ鍵ENCCK1=Enc(DK1, CK)を生成し、装置識別子AID1に対応付ける。なお、Enc(K, P)を平文Pを暗号化鍵Kで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子(AID2、・・・、AIDs)とデバイス鍵(DK2、・・・、DKs)に対しても同様の処理を行い、暗号化コンテンツ鍵ENCCK2=Enc(DK2, CK)、・・・、ENCCKn=Enc(DKs, CK)を生成し、装

置識別子 A I D 2、・・・、A I D s に対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵の s 組から構成される、図 4 のような暗号化鍵束 K B を生成する。暗号化鍵束 K B をこのような構成にすることによって、各実行装置 1 2 はその暗号化鍵束 K B と自身の保持するデバイス鍵 (D K 1、・・・、D K s の何れか) を用いてコンテンツ鍵 C K が取得出来るようになる。そして、暗号化鍵束 K B を配布部 1 0 9 に出力する。なお、特許文献 2 などに記載の方法を用いることで、暗号化鍵束 K B の中の暗号化コンテンツ鍵 (先程の例では s 個) の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵 C K を取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部 1 0 4 で使用する暗号アルゴリズムは、例えば、非特許文献 1 に記載の A E S 方式 (128 ビット鍵) などであり、実行装置 1 2 のコンテンツ鍵取得部 1 2 3 と同じ暗号アルゴリズムを用いる。

【0060】

(5) 暗号化部 105

暗号化部 105 は、入力部 101 からコンテンツ C N T を入力され、さらに、コンテンツ鍵生成部 102 からコンテンツ鍵 C K とが入力された場合、以下のようにして暗号化コンテンツ E N C C N T を生成する。ここで、コンテンツ C N T は、図 5 で示すように、n 個 (n は 2 以上の自然数) の部分コンテンツ C N T # 1、C N T # 2、C N T # 3、・・・、C N T # n から構成されるとする。なお、コンテンツ C N T は、初めから n 個に分割されているとする。コンテンツ C N T が初めから n 個に分割されている一例としては、コンテンツ C N T が複数のファイルから構成されている場合が挙げられる。例えば、コンテンツ C N T が D V D - V I D E O 形式の動画コンテンツの場合、V O B (V i d e o O B j e c t) ファイル等で分割されており、コンテンツ C N T が複数の M P E G 2 形式の動画コンテンツから構成されている場合や、複数の M P 3 形式の音声コンテンツから構成されている場合もある。なお、D V D - V i d e o 形式については、例えばインターネットアドレス <http://positron.jfet.org/dvdvideo.html> に記載されており、M P E G 形式については、例えばインターネットアドレス <http://www.pioneer.co.jp/crdl/tech/mpeg/1.html> に記載されている。

【0061】

そして、コンテンツ鍵 C K を用いて部分コンテンツ C N T # 1 を暗号化し、暗号化部分コンテンツ E N C C N T # 1 = E n c (C K, C N T # 1) を生成する。続いて、同じコンテンツ鍵 C K を用いて部分コンテンツ C N T # 2 を暗号化し、暗号化部分コンテンツ E N C C N T # 2 = E n c (C K, C N T # 2) を生成する。これを繰り返して、図 5 で示すような n 個の暗号化部分コンテンツ E N C C N T # 1、・・・、E N C C N T # n から構成される暗号化コンテンツ E N C C N T を生成する。暗号化部 105 で使用する暗号アルゴリズムは、例えば、非特許文献 1 に記載の A E S 方式 (128 ビット鍵) などであり、実行装置 1 2 の実行部 1 2 6 と同じ暗号アルゴリズムを用いる。ここでは暗号化コンテンツ E N C C N T の生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵 C K で暗号化していたが、非特許文献 1 に記載のブロック暗号のモードを利用してもよい。例えば、C B C モードや O F B モード、C F B モードなどでもよく、さらに、ある一定間隔毎にモード (例: C B C モード) の初期値を変化させるようにしたものでも良い。

【0062】

続いて、n 個の暗号化部分コンテンツのそれぞれを識別、特定出来る、n 個の特定情報 A D D R # 1、・・・、A D D R # n を取得する。この n 個の特定情報は、例えば、暗号化コンテンツ E N C C N T が複数のファイルから構成されている場合、各ファイルの先頭の論理アドレスとサイズ、もしくは、先頭と終端の論理アドレス、もしくは、先頭の物理アドレスとサイズ、もしくは、先頭と終端の物理アドレス、などである。ここでは、暗号化部分コンテンツ E N C C N T # 1 を識別、特定する情報を特定情報 A D D R # 1、暗号化部分コンテンツ E N C C N T # 2 を識別、特定する情報を特定情報 A D D R # 2、暗号化部分コンテンツ E N C C N T # 3 を識別、特定する情報を特定情報 A D D R # 3、・・・、暗号化部分コンテンツ E N C C N T # n を識別、特定する情報を特定情報 A D D R #

nとする。そして、暗号化コンテンツ ENCCNT を配布部 109 へ出力し、暗号化部分コンテンツと特定情報の n 組 {ENCCNT#1、ADDR#1}、{ENCCNT#2、ADDR#2}、・・・、{ENCCNT#n、ADDR#n} を、ヘッダ情報生成部 106 へ出力する。

【0063】

なお、それぞれの特定情報は、上記で紹介した情報に限らず、各暗号化部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。

【0064】

(6) ヘッダ情報生成部 106

ヘッダ情報生成部 106 は、暗号化部 105 から、暗号化部分コンテンツと特定情報の n 組 {ENCCNT#1、ADDR#1}、{ENCCNT#2、ADDR#2}、・・・、{ENCCNT#n、ADDR#n} とが入力された場合、以下のようにして、ヘッダ情報 HEAD 及びコンテンツ位置情報 POS を生成する。

【0065】

n 組の暗号化部分コンテンツと特定情報からヘッダ情報 HEAD を生成する大まかな流れは、図 6 で示す通りである。まず、n 個の暗号化部分コンテンツのそれぞれに対して、第一ハッシュテーブル HASHTBL1#1、HASHTBL1#2、・・・、HASHTBL1#n を生成する。そして、n 個の第一ハッシュテーブル及び特定情報を用いて第二ハッシュテーブル HASHTBL2 及びコンテンツ位置情報 POS を生成する。

【0066】

まず、n 個の暗号化部分コンテンツのそれぞれに対して、第一ハッシュテーブルを生成する方法について説明する。ここでは例として、暗号化部分コンテンツ ENCCNT#1 から第一ハッシュテーブル HASHTBL1#1 を生成する方法について説明する。なお、暗号化部分コンテンツ ENCCNT#2、・・・、ENCCNT#n から第一ハッシュテーブル HASHTBL1#2、・・・、HASHTBL1#n のそれぞれを生成する方法は、暗号化部分コンテンツ ENCCNT#1 から第一ハッシュテーブル HASHTBL1#1 を生成する方法と同じであるため、説明を省略する。まず、図 7 で示すように、暗号化部分コンテンツ ENCCNT#1 を m 個 (m は 1 以上の自然数) のユニット U#1、U#2、・・・、U#m に分割する。分割する方法の一例としては、例えば暗号化部分コンテンツをある所定の区切り毎に分割する方法がある。ある所定の区切り方の具体例としては、コンテンツデータが DVD-VIDEO 形式の動画コンテンツの場合、例えば、セル (Cell) 単位などである。コンテンツデータが MPEG2 形式の動画コンテンツの場合、例えば、GOP 単位、フィールド単位、フレーム単位、I ピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長 (ECC ブロック単位) などである。また、コンテンツデータの形式を問わず、例えば、64 キロバイト単位、1 メガバイト単位、1 秒単位、1 分単位などでも良い。そして、m 個のユニットのそれぞれを識別可能な第一識別子を取得、もしくは、生成する。第一識別子を取得、もしくは、生成する方法としては、各ユニットを識別可能な論理アドレスや物理アドレスを取得する方法や、自然数を順番に生成し割り当てていく (1、2、・・・、m) 方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した第一識別子をそれぞれ、ID1#1、ID1#2、・・・ID1#m とし、次のように第一識別子とユニットが対応しているとする。{ID1#1、U#1}、{ID1#2、U#2}、・・・、{ID1#m、U#n}。続いて、m 組の第一識別子とユニットの各組に対して、ユニットの属性値として第一ハッシュ値を計算する。ユニットの第一ハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献 1 に記載の SHA-1 アルゴリズムやブロック暗号を用いた CBC-MAC などがあり、実行装置 12 の認証情報検証部 125 で用いる方法と同じものを用いる。ここで、各組に対して計算した第一ハッシュ値をそれぞれ、HASH1#1、HASH1#2、・・・、HASH1#m とし、次のように第一識別子とユニットと第一ハッシュ値が対応しているとする

。 {ID1#1、U#1、HASH1#1}、{ID1#2、U#2、HASH1#2}、
・・・、{ID1#m、U#m、HASH1#m}。最後に、その中から第一識別子と
第一ハッシュ値を抜き出し、第一ハッシュテーブルHASH TBL#1 = {ID1#1、
HASH1#1}、{ID1#2、HASH1#2}、・・・、{ID1#m、HASH
1#m} を生成する。

【0067】

続いて、n個の第一ハッシュテーブルと対応するn個の特定情報を用いて第二ハッシュ
テーブルHASH TBL2を生成する方法について、図8を用いて説明する。まず、n組
の特定情報と第一ハッシュテーブルのそれぞれに対して、第一ハッシュテーブルの属性値
として第二ハッシュ値を計算する。第一ハッシュテーブルの第二ハッシュ値を求める方法
としては、例えばm個の第一ハッシュ値と第一識別子の値を連結した値を一方方向性関数に
入力した場合の出力値を用いる方法があり、非特許文献1に記載のSHA-1アルゴリズム
やブロック暗号を用いたCBC-MACなどがあり、実行装置12の認証情報検証部1
25で用いる方法と同じものを用いる。ここで、各組に対して計算した第二ハッシュ値を
それぞれ、HASH2#1、HASH2#2、・・・、HASH2#nとし、次のように
特定情報と第一ハッシュテーブルと第二ハッシュ値が対応しているとする。{ADDR#
1、HASH TBL1#1、HASH2#1}、{ADDR#2、HASH TBL1#2
、HASH2#2}、・・・、{ADDR#n、HASH TBL1#n、HASH2#n
}。その中から特定情報と第二ハッシュ値を抜き出し、第二ハッシュテーブルHASH T
BL2 = {ADDR#1、HASH2#1}、{ADDR#2、HASH2#2}、..
、{ADDR#n、HASH2#n} を生成する。

【0068】

最後に、n個の特定情報を用いてコンテンツ位置情報POSを生成する方法について、
図9を用いて説明する。それぞれの特定情報ADDR#1、ADDR#2、・・・、AD
DR#nに対して、対応する暗号化部分コンテンツをユニット単位で分割した個数である
ユニット数をそれぞれNUMU#1、NUMU#2、・・・、NUMU#nとする。そし
て、そのn組の特定情報とユニット数から構成される、コンテンツ位置情報POS = {A
DDR#1、NUMU#1}、{ADDR#2、NUMU#2}、・・・、{ADDR#
n、NUMU#n} を生成する。

【0069】

そして、n個の第一ハッシュテーブルHASH TBL1#1、HASH TBL1#2、
・・・、HASH TBL1#n及び第二ハッシュテーブルHASH TBL2から構成され
るヘッダ情報HEADを生成し、コンテンツ位置情報POSとともに、配布部109へ出
力する。また、第二ハッシュテーブルHASH TBL2及びコンテンツ位置情報POSを
認証情報生成部108へ出力する。

【0070】

(7) 認証情報生成情報格納部107

認証情報生成情報格納部107は、ヘッダ情報HEADの認証情報である認証情報AU
THを生成するための、認証情報生成情報GENAUTHを予め与えられ、保持するもの
である。この認証情報生成情報GENAUTHは、例えば、デジタル署名アルゴリズムの
署名生成鍵（秘密鍵）である。認証情報生成情報GENAUTHに対応する検証情報VE
Rは、実行装置12の検証情報格納部124に格納されている。この検証情報VERは、
例えば、デジタル署名アルゴリズムの署名検証鍵（公開鍵）である。デジタル署名アルゴ
リズムは、例えば、非特許文献1に記載のDSA方式やRSA署名などである。

【0071】

(8) 認証情報生成部108

認証情報生成部108は、ヘッダ情報生成部106から第二ハッシュテーブルHASH
TBL2及びコンテンツ位置情報POSが入力された場合、以下のようにして、認証情報
AUTHを生成する。まず、認証情報生成情報格納部107にアクセスして、認証情報生
成情報GENAUTHを取得する。そして、図10で示すように、第二ハッシュテーブル

HASHTBL 2 及びコンテンツ位置情報 POS に含まれる値と認証情報生成情報 GENAUTH を用いて、認証情報である認証情報 AUTH を生成する。なお、認証情報 AUTH の生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。ここでは、デジタル署名アルゴリズムを用いる方法の一例を説明する。まず、第二ハッシュテーブル HASHTBL 2 に含まれる n 個の第二ハッシュ値と n 個の特定情報と、コンテンツ位置情報 POS に含まれる n 個の特定情報と n 個のユニット数を結合した値に対するデジタル署名を作成する。ここで、GENSIG (K, M) は署名生成鍵 K を用いてメッセージ M に対して生成されたデジタル署名とすると、認証情報 AUTH は、 $AUTH = GENSIG (GENAUTH, \{HASH2\#1 || ADDR\#1 || NUMU\#1\} || \{HASH2\#2 || ADDR\#2 || NUMU\#1\} || \dots || \{HASH2\#n || ADDR\#n || NUMU\#n\})$ となる。そして、認証情報 AUTH を配布部 109 へ出力する。なお、認証情報生成部 108 で使用するデジタル署名アルゴリズムは、実行装置 12 の認証情報検証部 125 で用いるデジタル署名アルゴリズムと同じものを用いる。

【0072】

(9) 配布部 109

配布部 109 は、暗号化鍵束生成部 104 から入力された暗号化鍵束 KB と、暗号化部 105 から入力された暗号化コンテンツ ENCCNT と、ヘッダ情報生成部 106 から入力されたヘッダ情報 HEAD 及びコンテンツ位置情報 POS と、認証情報生成部 108 から入力された認証情報 AUTH と、を可搬媒体 11 へ記録するものである。例えば、可搬媒体 11 が書き込み可能な光ディスクであり、配布部 109 は書き込み用レーザー等を用いて該当データを記録する。

【0073】

<配布センタ 10 の動作>

以上で、配布センタ 10 の構成について説明を行ったが、ここでは配布センタ 10 の動作の一例について、図 11 に示すフローチャートの処理を行う。なお、配布センタ 10 の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【0074】

入力部 101 は、外部から入力されたコンテンツ CNT をコンテンツ鍵生成部 102 へ出力し、コンテンツ鍵生成要求 REQ をコンテンツ鍵生成部 102 へ出力する (ステップ S101)。

【0075】

コンテンツ鍵生成要求 REQ を入力されたコンテンツ鍵生成部 102 は、コンテンツ鍵 CK を生成し、コンテンツ鍵 CK を暗号化鍵束生成部 104 及び暗号化部 105 へ出力する (ステップ S102)。

【0076】

コンテンツ鍵 CK を入力された暗号化鍵束生成部 104 は、実行装置情報格納部 103 にアクセスして複数の実行装置 12 が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵 CK とを基に、暗号化鍵束 KB を生成する。そして、暗号化鍵束 KB を配布部 109 に出力する (ステップ 103)。

【0077】

コンテンツ CNT 及びコンテンツ鍵 CK が入力された暗号化部 105 は、コンテンツ鍵 CK を基に、コンテンツ CNT を暗号化し、暗号化コンテンツ ENCCNT を生成する。そして、暗号化コンテンツ ENCCNT を配布部 109 へ出力し、 n 組の暗号化部分コンテンツと特定情報を、ヘッダ情報生成部 106 へ出力する (ステップ S104)。

【0078】

n 組の暗号化部分コンテンツと特定情報を入力されたヘッダ情報生成部 106 は、 n 個の第一ハッシュテーブル HASHTBL 1 # 1、 \dots 、HASHTBL 1 # n と第二ハッシュテーブル HASHTBL 2 からなるヘッダ情報 HEAD、及びコンテンツ位置情報 POS を生成する。そして、ヘッダ情報 HEAD 及びコンテンツ位置特定情報 POS を配

布部 109 へ出力し、さらに、第二ハッシュテーブル H A S H T B L 2 とコンテンツ位置情報 P O S を認証情報生成部 108 へ出力する（ステップ S 105）。

【0079】

第二ハッシュテーブル H A S H T B L 2 とコンテンツ位置情報 P O S を入力された認証情報生成部 108 は、認証情報生成情報格納部 107 にアクセスして、認証情報生成情報 G E N A U T H を取得する。そして、認証情報生成情報 G E N A U T H を用いて、第二ハッシュテーブル H A S H T B L 2 とコンテンツ位置情報 P O S に対する認証情報である認証情報 A U T H を生成する。そして、認証情報 A U T H を配布部 109 へ出力する（ステップ S 106）。

【0080】

配布部 109 は、入力された暗号化鍵束 K B とヘッダ情報 H E A D と認証情報 A U T H と暗号化コンテンツ E N C C N T とを可搬媒体 11 へ記録する（ステップ S 107）。

【0081】

以上が、不正コンテンツ検知システム 1 の構成要素である配布センタ 10 の構成と動作である。続いて、可搬媒体 11 の構成について説明を行う。

【0082】

＜可搬媒体 11 の構成＞

可搬媒体 11 は、例えば、DVD-ROM や CD-ROM 等のような光ディスクの媒体（メディア）であり、図 12 に示すように、暗号化鍵束 K B とヘッダ情報 H E A D とコンテンツ位置情報 P O S と認証情報 A U T H と暗号化コンテンツ E N C C N T とが配布センタ 10 によって記録されているものとする。

【0083】

以上が、不正コンテンツ検知システム 1 の構成要素である可搬媒体 11 の構成である。続いて、実行装置 12 の構成と動作について説明を行う。

【0084】

＜実行装置 12 の構成＞

実行装置 12 は、図 13 に示すように、取得部 121、デバイス鍵格納部 122、コンテンツ鍵取得部 123、検証情報格納部 124、認証情報検証部 125、実行部 126 とから構成される。

【0085】

（1）取得部 121

取得部 121 は、可搬媒体 11 に記録されているデータの読み取りを行う。取得部 121 は、実行装置 12 が可搬媒体 11 のデータを読み取り可能になった場合に、可搬媒体 11 に記録されている暗号化鍵束 K B 及びコンテンツ位置情報 P O S 及び認証情報 A U T H を取得し、暗号化鍵束 K B をコンテンツ鍵取得部 123 へ出力し、コンテンツ位置情報 P O S と認証情報 A U T H を認証情報検証部 125 へ出力する。また、取得部 121 は、認証情報検証部 125 及び実行部 126 からの要求により、可搬媒体 11 に記録されているヘッダ情報 H E A D 及び暗号化コンテンツ E N C C N T の全部、もしくは、一部を取得できるものである。

【0086】

（2）デバイス鍵格納部 122

デバイス鍵格納部 122 は、配布センタ 10 の実行装置情報格納部 103 の中の鍵情報の一部を保持するものであり、デバイス鍵格納部 122 に与えられる鍵情報と暗号化鍵束 K B を用いて、コンテンツ鍵 C K が取得出来るものである。例えば、実行装置情報格納部 103 が図 3 のような場合、デバイス鍵格納部 122 には、装置識別子 A I D i とデバイス鍵 K i （i は 1 から s のいずれか）が与えられる。

【0087】

（3）コンテンツ鍵取得部 123

コンテンツ鍵取得部 123 は、取得部 121 から暗号化鍵束 K B が入力された場合、デバイス鍵格納部 122 に格納されている鍵情報及び暗号化鍵束 K B を用いて、コンテンツ

鍵CKを取得する。例えば、暗号化鍵束KBが図4のような場合で、デバイス鍵格納部122には装置識別子AIDiとデバイス鍵DKi(iは1からsのいずれか)が与えられている場合、コンテンツ鍵取得部123はデバイス鍵格納部122から装置識別子AIDiとデバイス鍵DKiを取得し、暗号化鍵束KBの中から装置識別子AIDiに対応する暗号化コンテンツ鍵ENCCKi(ENCCK1からENCCKsの何れか)を取得する。そしてデバイス鍵DKiを基に、暗号化コンテンツ鍵ENCCKiを復号化することによって、コンテンツ鍵CK=Dec(DKi, ENCCKi)を取得する。なお、Dec(K, C)は暗号文Cを復号化鍵Kを用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵CKを実行部126へ出力する。

【0088】

(4) 検証情報格納部124

検証情報格納部124は、認証情報AUTHの正当性を検証するために必要な検証情報VERを保持するものである。この検証情報VERに対応する認証情報生成情報GENAUTHは、配布センタ10の認証情報生成情報格納部107に格納されている。例えば、検証情報VERはデジタル署名アルゴリズムの署名検証鍵(公開鍵)である。

【0089】

(5) 認証情報検証部125

認証情報検証部125は、コンテンツ位置情報POS及び認証情報AUTHが入力された場合、認証情報AUTHの正当性を検証する。検証は以下のように行われる。

【0090】

まず、図14で一例を示すように、コンテンツ位置情報POSに含まれるn組の特定情報ADDR#1、・・・、ADDR#nとユニット数U#1、・・・、U#nから、i組(iは1以上n-1以下の自然数)の特定情報とユニット数を選択する。ここで、選択されたi組の特定情報とユニット数からなるデータを被選択コンテンツ位置情報とする。ここでは、第三者によってどの特定情報とユニット数が選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、認証情報検証部125が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献2が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、認証情報検証部125が温度センサや湿度センサを有することにより実現出来る。

【0091】

続いて、図15で示すように、選択されたi組の特定情報とユニット数(被選択コンテンツ位置情報)、及び、可搬媒体11に記録されている第二ハッシュテーブルHASH TBL2の一部を基に、入替第二ハッシュテーブルREPHASHTBL2を生成する。入替第二ハッシュテーブルREPHASHTBL2を生成する方法は、以下の通りである。まず、選択されたi組の特定情報とユニット数のそれぞれに対応するi個の入替第一ハッシュテーブルを生成する。ここでは、選択されたi組の特定情報とユニット数のうち、1組が特定情報ADDR#1とユニット数NUMU#1である場合を例に挙げ、入替第一ハッシュテーブルREPHASHTBL1#1を生成する手順について説明する。なお、他の特定情報とユニット数の場合であっても、同様の手順となる。まず、ユニット数NUMU#1を基に、特定情報ADDR#1に対応する暗号化部分コンテンツENC CNT#1に含まれるユニットの数を認識し、1番目からd番目(dはユニット数NUMU#1)までのユニットのうち、j個(jは1以上m以下の自然数)のユニットを選択する。ここでも、第三者によってどのユニットが選択されるか推測できないようにする。この方法は、先ほど、コンテンツ位置情報POSに含まれるn組の特定情報とユニット数から、i組の特定情報とユニット数を選択する方法と同様の方法が利用可能であるため、説明を省略する。以後、説明を簡略化するために、jは1とし、図16で示すように、ユニットU#3(図16における横点線)が選択されたとする。そして、そのユニットU#3に対する属

性値である第一ハッシュ値H1（図16における縦線）を計算する。また、特定情報ADDR#1及びユニット数U#3を基に、取得部121経由で可搬媒体11からID1#3以外の選択されなかった第一識別子に対応する第一ハッシュ（図16における横点線）を取得する。そして、選択された第一識別子に対応するユニットの属性値を計算することによって取得した第一ハッシュ値、及び、選択されなかった第一識別子に対応する第一ハッシュ値から構成される、図16で示される、入替第一ハッシュテーブルREPHASHTBL1#1を生成する。

【0092】

続いて、生成されたi個の入替第一ハッシュテーブル、及び、可搬媒体11に記録されている第二ハッシュテーブルHASHTBL2の一部を基に、入替第二ハッシュテーブルREPHASHTBL2を生成する方法について説明する。図17で一例を示すように、まず、i個の入替第一ハッシュテーブルのそれぞれに対する属性値として、第二ハッシュ値（図17における縦線）を生成する。図17では、入替第一ハッシュテーブルREPHASHTBL1#1に対する属性値として第二ハッシュ値H2#1、・・・、入替第一ハッシュテーブルREPHASHTBL1#cに対する属性値として第二ハッシュ値H2#cとしている。次に、選択されなかった特定情報に対応する第二ハッシュ値を、取得部121経由で可搬媒体11から取得する（図17における横点線）。そして、入替第一ハッシュテーブルの属性値を計算することによって取得した第二ハッシュ値、及び、選択されなかった特定情報に対応する第二ハッシュ値から構成される、図17で示される、入替第二ハッシュテーブルREPHASHTBL2を生成する。

【0093】

最後に、検証情報格納部124に格納されている検証情報VERを使って、図18で示すように、認証情報AUTHが発行センタ10による入替第二ハッシュテーブルREPHASHTBL2及びコンテンツ位置情報POSに対する正規の認証情報であるかを検証する。例えば、デジタル署名検証アルゴリズムを用いて、認証情報AUTHが正しいデジタル署名であるかを検証する。このデジタル署名検証アルゴリズムは、配布センタ10の認証情報生成部108で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献1に記載のDSA方式などである。認証情報検証部125は、認証情報AUTHが発行センタ10による正しい認証情報である場合にのみ、実行開始許可情報PERMを実行部126へ出力する。なお、被選択コンテンツ位置情報に含まれるi個の特定情報に対応するi個の暗号化部分コンテンツを、被選択部分コンテンツとする。

【0094】

(6) 実行部126

実行部126は、コンテンツ鍵取得部123からコンテンツ鍵CKが入力され、かつ、認証情報検証部125から実行開始許可情報PERMが入力された場合に、取得部121経由で、可搬媒体11に記録されている暗号化コンテンツENCNTを逐次取得し、逐次コンテンツ鍵CKを基に復号化を行って、逐次実行するものである。例えば、実行部126はMPEG2データやMP3データをデコードする機能を有するデコータを有していて、MPEG2形式の動画コンテンツやMP3形式の音声コンテンツであるコンテンツCNTを逐次デコードして、外部に出力するものである。また、例えば、実行部126は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生するようなものでも良いし、別の可搬媒体や記録媒体にコンテンツデータを出力するようなものでも良いし、印刷機能を有しコンテンツデータを紙などに印刷するようなものでもよい。

【0095】

<実行装置12の動作>

以上で、実行装置12の構成について説明を行ったが、ここで実行装置12の動作について、図19に示すフローチャートを用いて説明する。なお、実行装置12の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【0096】

実行装置12が可搬媒体11のデータを読み取り可能になった場合に、取得部121は可搬媒体11に記録されている暗号化鍵束KB及びコンテンツ位置情報POS及び認証情報AUTHを取得し、暗号化鍵束KBをコンテンツ鍵取得部123へ出力し、コンテンツ位置情報POSと認証情報AUTHを認証情報検証部125へ出力する（ステップS121）。

【0097】

暗号化鍵束KBを入力されたコンテンツ鍵取得部123は、デバイス鍵格納部122が保持している鍵情報を用いて、コンテンツ鍵CKを取得する。そして、コンテンツ鍵CKを実行部126へ出力する（ステップS122）。

【0098】

コンテンツ位置情報POSと認証情報AUTHを入力された認証情報検証部125は、検証情報格納部124に格納されている検証情報VERを使って、認証情報AUTHが発行センタ10による正規の認証情報であるかを検証する（ステップS123）。

【0099】

認証情報検証部125は、認証情報AUTHが発行センタ10による正しい認証情報である場合にのみ、実行開始許可情報PERMを実行部126へ出力し、ステップS125へ進む。もし、認証情報AUTHが正しい認証情報ではない場合、処理を終了する（ステップS124）。

【0100】

コンテンツ鍵CK及び実行開始許可情報PERMを入力された実行部126は、取得部121経由で、可搬媒体11に記録されている暗号化コンテンツENCCNTを逐次取得し、逐次コンテンツ鍵CKを基に復号化を行って、逐次実行する（ステップS125）。

【0101】

以上が、不正コンテンツ検知システム1の構成要素である実行装置12の構成と動作である。尚、デバイス鍵格納部122、コンテンツ鍵取得部123、検証情報格納部124、認証情報検証部125、等の各機能ブロックは典型的には集積回路であるLSIとして実現されていてもよい。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

【0102】

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

【0103】

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用して良い。

【0104】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

【0105】

<不正コンテンツ検知システム1の効果>

以上、不正コンテンツ検知システム1について実施の形態に基づいて説明したが、この不正コンテンツ検知システム1においては、配布センタ10が、暗号化されたコンテンツCNTとともに、ヘッダ情報HEAD、及び、コンテンツ位置情報POS、及び、認証情報AUTH（例えばデジタル署名）を可搬媒体11に記録するようにして、実行装置12では、コンテンツCNTの実行、再生開始前に、認証情報AUTHが正規の認証情報（例えばデジタル署名）であるか検証する際に、コンテンツ位置情報POSを基にヘッダ情報HEADに含まれるハッシュ値のうち、一部のハッシュ値に絞って検証するようにした。

ここでは、コンテンツCNTを実行、再生開始する毎に、異なるハッシュ値を選択するようにして、不正者は、どのハッシュ値が選択されるか予想出来ないように注意する。そして、選択された一部のハッシュ値が共に正当であると検証された場合にのみ、コンテンツCNTの実行、再生を開始するようにした。そうすることにより、実行装置12は、不正な認証情報AUTHもしくはヘッダ情報HEADもしくはコンテンツ位置情報POSもしくは暗号化コンテンツENCCNTが記録された可搬媒体11のコンテンツCNTは実行開始しないようになる。これにより、コンテンツCNTの中のある部分コンテンツを不正な部分コンテンツに差し替えようとしても、その不正な部分コンテンツに差し替えられた部分に対応するハッシュ値の検証が行われた場合、そのコンテンツは実行出来なくなる。つまり、コンテンツCNTの一部分でも不正な部分コンテンツに差し替えた場合、ある確率でコンテンツCNTを実行できなくなることになる。これは、コンテンツCNTの中の一部を、不正なコンテンツに差し替えられるような攻撃を防ぐ抑止力となる。

【0106】

さらに、実行装置12は、認証情報AUTHの正当性の検証を、コンテンツCNTを実行、再生開始する前に全て行うため、コンテンツCNTの実行、再生中の特別な処理が必要なくなり、従来例に比べ、コンテンツCNTの実行中の処理負荷が軽減されるという効果を有する。

【0107】

さらに、第一ハッシュテーブルと第二ハッシュテーブルというハッシュの2層構造にすることによって、実行装置12では、認証情報AUTHの検証時に、可搬媒体11から全ての第一ハッシュ値を取得する必要がなくなった。これにより、可搬媒体から取得しなくてはならないハッシュ値の数を少なくすることが出来、実行装置12の処理時間を短くすることが出来る。

【0108】

また、さらに、実行装置12では、認証情報AUTHを用いて、コンテンツ位置情報POSの正当性を検証するようにした。これにより、可搬媒体11におけるファイルシステム等を操作することによって、実行装置12の認証情報検証部125において選択対象となる特定情報及びユニットの数を意図的に少なくするような攻撃に耐性を持たせることが出来るようになった。実行装置12の認証情報検証部125において選択対象となる特定情報及びユニットの数を意図的に少なく出来る場合、その選択対象外となった特定情報及びユニットに対応するコンテンツを不正コンテンツに差し替えることが可能となる。そのため、コンテンツ位置情報POSの正当性を検証することは、実行装置12の認証情報検証部125において選択対象となる特定情報及びユニットの数を意図的に少なく出来ないという面で効果がある。

【0109】

また、さらに、実行装置12では、コンテンツを実行、再生開始する場合に、暗号化コンテンツの一部分の属性値（ハッシュ値）を検証するようにした。これにより、従来技術のように、暗号化コンテンツを一度復号化して属性値を検証する場合に比べ、処理時間を短縮することが出来た。

【0110】

<変形例>

上記に説明した実施の形態は、本発明の実施の形態の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

【0111】

(1) 実施の形態1の認証情報AUTHは、第二ハッシュテーブルHASHTBL2及びコンテンツ位置情報POSを連結した値に対する認証情報であったが、これに限るものではない。例えば、第二ハッシュテーブルHASHTBL2に含まれるn個の第二ハッシュ値とコンテンツ位置情報POSに含まれるn個の特定情報とn個のユニット数を連結した値に対する認証情報であっても良い。また、第二ハッシュテーブルHASHTBL2に

含まれる n 個の第二ハッシュ値とコンテンツ位置情報 P O S に含まれる n 個のユニット数を連結した値に対する認証情報であっても良い。

【0112】

(2) 実施の形態 1 の認証情報 A U T H は、第二ハッシュテーブル H A S H T B L 2 及びコンテンツ位置情報 P O S を連結した値に対する認証情報であったが、これに限るものではない。例えば、第二ハッシュテーブル H A S H T B L 2 及びコンテンツ位置情報 P O S に加え、コンテンツ鍵 C K を連結した値に対する認証情報であっても良い。こうすることにより、コンテンツ鍵 C K を持たないものは、認証情報 A U T H の正当性すら検証出来なくなり、安全性がより高まる。

【0113】

(3) 実施の形態 1 の可搬媒体 11 では、暗号化コンテンツ E N C C N T が記録されていたが、可搬媒体 11 には、暗号化されていないコンテンツ C N T をそのまま記録するようにしても良い。こうすることにより、実行装置 12 で暗号化コンテンツ E N C C N T を復号化する必要がなくなるという効果が生まれる。

【0114】

(4) 実施の形態 1 の配布センタ 10 は、図 2 で示すような構成に限るものではない。例えば、認証情報 A U T H などを可搬媒体 11 へ記録する配布部 109 と、ヘッダ情報 H E A D に対する認証情報を生成する認証情報生成部 108 とを、別の主体が行うようにしても良い。例えば、コンテンツ C N T に対する認証情報を生成するのはコンテンツ C N T の正規の著作権者であり、認証情報 A U T H などを可搬媒体 11 へ記録するのはディスク製造業者であるなど、が考えられる。

【0115】

(5) 実施の形態 1 の配布センタ 10 の認証情報生成情報格納部 107、及び、実行装置 12 の検証情報格納部 125 は、これに限るものではない。例えば、以下のような例が考えられる。

【0116】

(i) 一つの例として、認証情報生成情報格納部 107 は、図 20 で示すように、1 つの認証情報生成情報 G E N A U T H i (G E N A U T H 1、 \dots 、G E N A U T H w のいずれか (w は 1 以上の自然数)) と対応する検証情報識別子 V E R I D i を保持しており、検証情報格納部 125 は、図 21 で示すように、 w 組の検証情報識別子 (G E N A U T H 1、 \dots 、G E N A U T H w) と、その検証情報識別子に対応する認証情報生成情報と対となる検証情報 (V E R 1、 \dots 、V E R w) を保持している場合が考えられる。この場合、配布センタ 10 の配布部 109 は、可搬媒体 11 に、認証情報生成情報格納部 107 に格納されている検証情報識別子 G E N A U T H i を加えて記録するようにして、さらに、実行装置 12 の認証情報検証部 126 は、可搬媒体 11 に記録されている検証情報識別子 G E N A U T H i に対応する検証情報 V E R i (V E R 1、 \dots 、V E R w のいずれか) を検証情報格納部 125 から取得し、その検証情報 V E R i を基に、認証情報 A U T H を検証することになる。

【0117】

(i i) 別の例として、認証情報生成情報格納部 107 には、認証情報生成情報 G E N A U T H と対応する検証情報 V E R を保持しており、検証情報格納部 125 には、何も保持していない場合が考えられる。この場合、配布センタ 10 の配布部 109 は、可搬媒体 11 に、認証情報生成情報格納部 107 に格納されている検証情報 V E R を加えて記録するようにして、さらに、実行装置 12 の認証情報検証部 126 は、可搬媒体 11 に記録されている検証情報 V E R を基に、認証情報 A U T H を検証することになる。

【0118】

(i i i) さらに別の例として、認証情報生成情報格納部 107 には、図 22 で示すように、認証情報生成情報 G E N A U T H と対応する検証情報 V E R、及び、第三者機関によって生成された検証情報 V E R に対する認証情報 (例えばセンタによるデジタル署名) であるセンタ認証情報 C A U T H を保持しており、検証情報格納部 125 は、図 23 で

示すように、第三者機関の検証情報であるセンタ検証情報CVER（例えばセンタのデジタル署名の署名検証鍵）を保持している場合が考えられる。なお、第三者機関の具体例としては、信頼出来る第三者機関（Trusted Third Party）や、鍵配布センタなどである。この場合、配布センタ10の配布部109は、可搬媒体11に、認証情報生成情報格納部107に格納されている検証情報VER及びセンタ認証情報CAUTHを加えて記録するようにして、さらに、実行装置12の認証情報検証部126は、検証情報格納部125のセンタ検証情報CVERを用いて、可搬媒体11に記録されているセンタ認証情報CAUTHが、検証情報VERに対する第三者機関の正規の認証情報であるかどうか検証し、その検証が成功した場合に、その検証情報VERを基に、認証情報AUTHを検証するようにすることになる。

【0119】

このようにすることによって、配布センタ10が複数存在している場合にそれぞれの配布センタ10に別の検証情報を設定したとしても、実行装置12に予め各検証情報を保持しておく必要がなくなる。

【0120】

(6) 変形例(5)において、実行装置12は、さらに、無効検証情報を外部から受信するようにしてもよい。例えば、変形例(5)の(i)の場合、無効検証情報には、検証情報識別子が含まれており、実行装置12には、外部から無効検証情報として検証情報識別子GENAUTHjを受信した場合に、検証情報格納部125に格納されている検証情報識別子GENAUTHjに対応する検証情報VERjを無効化する検証情報無効化部を備えていてもよい。

【0121】

また、変形例(5)の(ii)及び(iii)の場合、無効検証情報には、検証情報が含まれており、実行装置12の検証情報格納部125は、外部から受信した無効検証情報として検証情報を保持しており、認証情報検証部126は、検証情報格納部125の無効検証情報に、可搬媒体11に記録されている検証情報が含まれていないか確認を行い、含まれている場合は、コンテンツCNTの実行開始を行わないようにしてもよい。

【0122】

なお、実行装置12が外部から無効検証情報を受信する方法としては、可搬媒体11や記録媒体に記録されている無効検証情報を受信する方法や、通信ネットワークや放送網から無効検証情報をダウンロードする方法などがある。このようにすることによって、万が一、ある配布センタの認証情報生成情報が不正者に漏洩したとしても、その認証情報生成情報に対応する検証情報を無効検証情報に含めることによって、その漏洩した認証情報生成情報を無効化することが実現出来る。

【0123】

(7) 変形例(6)において、実行装置12は、最新の無効検証情報のみを検証情報格納部125に保持するようにしてもよい。例えば、無効検証情報には発行日が記載されており、実行装置12は、検証情報格納部125が保持する無効検証情報よりも発効日が新しい無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部125に上書きするようにしてもよいし、また、無効検証情報には発行IDが記載されており、実行装置12は、検証情報格納部125が保持する無効検証情報よりも発行IDが最新の無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部125に上書きするようにしてもよい。

【0124】

(8) 実施の形態1のコンテンツCNTは、動画データや音声データなどのコンテンツであったが、コンピュータプログラムであっても良い。この場合、実行装置12は、コンピュータプログラムを実行するために必要なCPUやメモリ、ディスクなどを備えていれば良い。こうすることにより、実行装置12では、不正なコンピュータプログラムを実行開始しないようになるため、コンピュータウイルス等を防ぐ対策として有効となる。

【0125】

(9) 実施の形態1の配布センタ10では、コンテンツ鍵生成部102においてコンテンツ鍵CKを生成していたが、配布センタ10が一以上のコンテンツ鍵CKを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵生成部102はコンテンツ鍵格納部からいずれかのコンテンツ鍵CKを取得するようにしても良い。こうすることにより、コンテンツ鍵CKを予めまとめて作成しておくことが出来る。

【0126】

(10) 実施の形態1の実行装置12のコンテンツ鍵取得部123では、暗号化鍵束KB、及びデバイス鍵格納部122に格納されている情報を用いて、コンテンツ鍵CKを取得していたが、配布センタ10がデバイス鍵格納部122の替わりに、コンテンツ鍵CKを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵取得部123はコンテンツ鍵格納部からコンテンツ鍵を取得するようにしても良い。この場合、発行センタ10は可搬媒体11に暗号化鍵束KBを記録する必要はなく、実行装置12は暗号化鍵束KBを受信する必要もない。こうすることにより、可搬媒体11に暗号化鍵束KBを記録しなくすむため、記録データのサイズを削減することが出来る。

【0127】

(11) 実施の形態1において、配布センタ10は、可搬媒体11を介して実行装置12へコンテンツCNTに関する情報を配布していたが、これに限るものではない。例えば、配布センタ10と実行装置12がインターネット等の通信ネットワークに接続されており、配布センタ10は、その通信ネットワークを介して実行装置12へコンテンツCNTに関する情報を配布してもよいし、他にも通信ネットワークが放送網であってもよい。

【0128】

(12) 実施の形態1において、実行装置12は可搬媒体11内のコンテンツCNTを実行開始する前に、そのコンテンツCNTが不正なものであるか検証していたが、これに限るものではない。例えば、可搬媒体11が光ディスクであり、実行装置12がディスクトレイを有している場合、可搬媒体11が実行装置12のディスクトレイに挿入された場合に、そのコンテンツCNTが不正なものであるか検証するようにしても良い。そうすることにより、ディスクトレイに挿入された可搬媒体11内のコンテンツCNTをイジェクトせずに何度も実行、再生する場合にでも、光ディスクの挿入時1度しか検証しないですむようになるため、コンテンツCNTの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体11がSDカード等の外部メモリで、実行装置12が外部メモリスロットを有している場合にも、同様のことが実現出来る。

【0129】

(13) 実施の形態1の実行装置12の認証情報検証部125においては、入替第二ハッシュテーブルを生成し、それを基に認証情報AUTHの正当性を検証していたが、これに限るものではない。例えば、実行装置12の認証情報検証部125では、まずステップ1として、図24で示すように、可搬媒体11に記録されていた認証情報AUTHが、同じく可搬媒体11に記録されていた第二ハッシュテーブル及びコンテンツ位置情報の正規の認証情報であるか検証し、次にステップ2として、図25で示すように、選択された特定情報に対応する暗号化部分コンテンツの属性値が、特定情報に対応する第二ハッシュ値と等しいかどうか検証し、さらに、選択された第一識別子に対応するユニットの属性値が、第一識別子に対応する第一ハッシュ値と等しいかどうか検証するようにしてもよい。これにより、同様にコンテンツの正当性を検証することが出来る。暗号化部分コンテンツの属性値と第二ハッシュ値との検証については、図26に詳細を示している。また、ユニットの属性値と第一ハッシュ値との検証については、図27に詳細を示している。

【0130】

(14) 実施の形態1において、可搬媒体11にはヘッダ情報HEADと暗号化コンテンツENCNTとをそれぞれ一つずつ格納していたが、これに限るものではない。例えば、可搬媒体11にはヘッダ情報HEADと暗号化コンテンツENCNTをそれぞれ z 個(z は2以上の自然数)格納しても良い。このような場合、以下のようなことが実現出来る。ここでは、例えば、可搬媒体11が光ディスクであり、実行装置12はディスク

レイを有しているとする。この場合、可搬媒体 11 が実行装置 12 のディスクトレイに挿入された時に、全てのヘッダ情報の中のコンテンツ位置情報からいくつかの特定情報を選択し検証を行うようにする。そして、複数あるコンテンツの中の一つのコンテンツを実行、再生開始する前に、そのコンテンツに対応するヘッダ情報の中のコンテンツ位置情報の中からいくつかの特定情報を選択し検証を行うようにしても良い。つまり、可搬媒体 11 が実行装置 12 のディスクトレイに挿入された場合に一度のみ、多くの数の特定情報の検証を行い、各コンテンツを実行、再生開始する際には、ディスクトレイに挿入された時よりも少ない数の特定情報に対して検証するようにする。これにより、ディスクトレイに挿入された可搬媒体 11 内のコンテンツを何度も実行する場合に、コンテンツの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体 11 は光ディスク出なくてもよく、例えば SD カード等の外部メモリであっても同様のことが実現出来る。

【0131】

(15) 実施の形態 1 においては、実行装置 12 の認証情報検証部 125 では、検証が成功した場合にのみ、実行部 126 へ実行許可情報 PERM を出力していたが、これに限るものではない。例えば、実行部 126 は、コンテンツ鍵取得部 123 からコンテンツ鍵を入力された場合に、可搬媒体 11 に記録された暗号化コンテンツを逐次取得、復号化、実行するようにして、認証情報検証部 125 は、検証が失敗した場合に、実行部 126 へ実行不許可情報 NOTPERM を出力するようにしてもよい。こうすることにより、コンテンツを実行開始するまでの時間を短縮することが出来るようになる。

【0132】

また、実行装置 12 の認証情報検証部 125 では、検証が成功した場合に実行部 126 へ実行許可情報 PERM を出力し、検証が失敗した場合に実行部 126 へ実行不許可情報 NOTPERM を出力するようにしてもよい。その際、実行不許可情報 NOTPERM を入力された実行部 126 では、外部に不正なコンテンツである旨メッセージを出力（例えば、ディスプレイに「不正なコンテンツです」と表示する）するようにしても良い。その際、実行不許可情報 NOTPERM を入力された実行部 126 では、暗号化コンテンツ ENCCNT の復号化及び実行、再生を停止するのではなく、暗号化コンテンツ ENCCNT の復号化及び実行、再生は通常通り行うが、同時に外部に警告を出力（例えば、ディスプレイに「警告：不正なコンテンツです」と表示する）するようにしても良い。また、実行装置 12 とサーバ（配布センタ 10 や別のセンタ）とが通信ネットワーク等で接続されていて、不正コンテンツである旨をそのサーバに通知するようにしてもよい。また、実行装置 12 では以後、あらゆる暗号化コンテンツ ENCCNT の復号化及び実行、再生を禁止するような状態になってもよい。また、実行装置 12 は、不正コンテンツを識別するコンテンツ識別情報（例えば、コンテンツ識別子）を装置内に記録するようにして、一定期間内、もしくは、永久的に、コンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、実行装置 12 は、同じコンテンツ識別情報（例えば、コンテンツ識別子）を持つコンテンツがある一定回数以上認証に失敗した場合、一定期間内、もしくは、永久的に、そのコンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、可搬媒体 11 が光ディスクであり、実行装置 12 がディスクトレイを有している場合、可搬媒体 11 がディスクトレイから排出されるようにしても良い。

【0133】

(16) 実施の形態 1 において、実行装置 12 の認証情報検証部 125 は、可搬媒体 11 から複数のユニットを取得する場合、アクセス時間の高速化を目的に、ユニットを取得する順番を最適化するようにしても良い。

【0134】

ここでは一例として、以下のような状況を想定する。実行装置 12 の認証情報検証部 125 は、4 個のユニット U#1、U#2、U#3、U#4 を取得したいとする。また、可搬媒体 12 は、CD-ROM や DVD-ROM などの光ディスクであるとする。その可搬

媒体 12 (光ディスク) 上には、データを記録する部分がいくつかに分かれており、年輪状に広がっている各領域をトラックと呼ぶ。各トラックには、いくつかのセクタを含み、データはセクタ単位で読み書きされる。例えば、1セクタのサイズは512バイトである。このような場合、可搬媒体 12 上の読み取り対象データは、トラック識別番号やセクタ識別番号やセクタサイズにより特定することが出来る。取得部 121 は、ヘッド機構部 (ピックアップ) 及び回転軸を備え、回転軸により可搬媒体 11 (光ディスク) を半時計回りに回転させるものとする。ヘッド機構部 (ピックアップ) から特定情報 (トラック識別番号やセクタ識別番号やセクタサイズ) を指定することで、対象部分のデータを取得出来るものとする。ここでは、4 個のユニット U#1、U#2、U#3、U#4 は、図 28 のように可搬媒体 12 (光ディスク) 上の位置に記録されているとし、可搬媒体 11 (光ディスク) とヘッド機構部も、図 28 で示す場所に存在しているとする。ここで、一般に、該当読取位置に対応するトラック位置へヘッド機構部 (ピックアップ) を移動させる時間がかかることが知られている。言い換えると、可搬媒体 11 (光ディスク) 上における内周のトラックから外周方向への移動、もしくは、外周のトラックから内周方向への移動に大きな処理時間がかかることに起因している。可搬媒体 11 (光ディスク) 上における内側のトラック上にあるデータを読み込んだ後に、外側のトラック上にあるデータを読み込み、その後、また内側のトラック上にあるデータを読み込む場合がその一例である。

【0135】

上記のような状況の場合、実施の形態 1 の動作に沿えば、まず 1 番目に、ユニット U#1 の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後、2 番目にユニット U#2 の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後も同様に、ユニット U#3 の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得し、最後に、ユニット U#4 の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。つまり、ユニット U#1 を取得するまでに、ヘッド機構部を内周から外周へ移動させ、続いて、ユニット U#2 を取得するまでに、ヘッド機構部を外周から内周へ移動させる。その後も、ユニット U#3 を取得するまでに、ヘッド機構部を内周から外周へ移動させ、最後に、ユニット U#4 を取得するまでに、ヘッド機構部を外周から内周へ移動させる。つまり、4 つのデータを取得するまでに、ヘッド機構部を何度も移動往復させる必要があることが分かる。

【0136】

そこで、本変形例では、上記全 4 つのデータの取得時間を短くする目的で、実行装置 12 の認証情報検証部 125 は、まずはじめに、それぞれのデータを取得する順序の最適値を計算する。例えば、一番初めに一番内側のトラック上にあるデータを全て取得して、その次に、一つ外側のトラック上にあるデータを全て取得いく、というようなことを繰り返す。この場合、トラック上に一つもデータがない場合は、そのトラックをスキップして次のトラックに進むようにする。例えば、4 つのユニットが図 28 のように可搬媒体 12 (光ディスク) 上の位置に記録されているとし、さらに、可搬媒体 11 (光ディスク) 及びヘッド機構部 (ピックアップ) が図 28 で示す場所に存在しているとする。すると、このデータを取得する順序の最適値は、内周側から外周側に向かって、ユニット U#2、ユニット U#4、ユニット U#3、ユニット U#1 となる。このようにすることで、可搬媒体 11 (光ディスク) 上に記録されているとびとびの部分データをランダムに取得する (いわゆるランダムアクセス) 場合にでも、取得したい全てのデータを取得するまでの時間を短縮することが出来る。なお、当然、ユニットは 4 個以外であっても適用可能である。

【0137】

なお、最適化手段は、取得部 121 (ヘッド機構部や回転軸等) の動作の特徴に依存するため、本変形例で説明した最適化手段は、あくまで一例であることを注意しておく。例えば、光ディスクの回転制御方式には、角速度一定方式や線速度一定方式があり、これらの特徴を考慮するようにしても良い。また、可搬媒体 11 は当然光ディスクでなくてもよく、例えばハードディスクなどでも同様のことが実現出来る。

【0138】

(17) 実施の形態1において、認証情報検証部125は、予め実行装置12に与えられているパラメータ*i*、*j*に従って検証を実施していたが、これに限るものではない。例えば、配信装置10は可搬媒体11に、パラメータ*i*、*j*の両方もしくは片方を記録するようにして、実行装置12は可搬媒体11に記録されているパラメータ*i*、*j*に従って検証するようにしてもよい。このパラメータ*i*、*j*は、多くすればセキュリティは向上するが、処理時間が多くなり、少なくすれば処理時間は少なくなるが、セキュリティは低下するという特徴を有する。つまり、本変形例を用いることで、コンテンツ配布者のポリシーに依存して、セキュリティレベルなどを設定することが出来るようになる。なお、実行装置12において、可搬媒体11にパラメータ*i*、*j*が記録されていない場合、予め与えられるデフォルトのパラメータ*i*、*j*を用いるようにしても良い。

【0139】

(18) 実施の形態1において、可搬媒体11には、さらに、不正なコンテンツかどうか検証するための情報を持たないコンテンツも同時に記録するようにしても良い。例えば、そのコンテンツの例としては、著作権保護等のセキュリティ技術の比較的必要のない映画のオープニング画面やDVDのメニュー画面などである。そして、実施形態1で説明した実行装置12による検証処理が終わるまで、それらコンテンツを実行するようにしても良い。それらコンテンツの例としては、違法コピーに関する警告文書、コンテンツ配給者のロゴやオープニング画面、DVDのメニュー画面などが挙げられる。なお、不正なコンテンツかどうか検証するための情報を持たないコンテンツは、予め実行装置12内に格納されていても良い。それらコンテンツの例としては、実行装置12が実行、再生可能なフォーマットのロゴや、実行装置12の製造メーカのロゴなどが挙げられる。

【0140】

(19) 実施の形態1において、暗号化部分コンテンツの属性値（ハッシュ値）の集合を第一ハッシュテーブルとして、全ての第一ハッシュテーブルに対する属性値（ハッシュ値）を第二ハッシュテーブルとして、認証情報AUTHはその第二ハッシュテーブルに対する認証情報としていたが、これに限るものではない。例えば、暗号化部分コンテンツの属性値（ハッシュ値）の集合を第一ハッシュテーブルとして、第一ハッシュテーブルをグループ分けし、その各グループの第一ハッシュテーブルを連結した値に対する属性値（ハッシュ値）を第二ハッシュテーブルとして、全ての第二ハッシュ値を連結した値に対する属性値（ハッシュ値）を第三ハッシュテーブルとして、認証情報AUTHはその第三ハッシュテーブルに対する認証情報としてもよい。この場合、ヘッダ情報HEADには、第一ハッシュテーブル及び第二ハッシュテーブル及び第三ハッシュテーブルを含めることになる。このようにすることによって、可搬媒体から取得しなくてはならないハッシュ値の数を少なくすることが出来、処理時間をさらに短くすることが出来る。なお、同様に、第四ハッシュテーブル以降を用いることも出来る。

【0141】

(20) 実施の形態1の可搬媒体11において記録されているデータに加え、さらに、可搬媒体に部分コンテンツの実行手順を記述したデータである実行手順データNAVを記録しており、実行装置12の実行部129では、その実行手順データNAVを基に、部分コンテンツを実行するような場合に、可搬媒体に、さらに、図29で示すように、その実行手順データNAVに対する認証情報として実行手順データ認証情報NAVAUTHを記録するようにして、認証情報検証部126では、その実行手順データ認証情報NAVAUTHが実行手順データNAVに対する正規の認証情報である場合にのみ、実行部129へ暗号化コンテンツENCCNT及びコンテンツ鍵CKを出力するようにしてもよい。ここで、実行手順データNAVは、例えば、DVD-VIDEO形式におけるナビゲーションファイル（拡張子がIFOのファイル）である。これにより、さらに強い不正コンテンツをも検知できる不正コンテンツ検知システムが実現出来る。

【0142】

(21) 実施の形態1において、可搬媒体12に記録されるヘッダ情報HEADは、見

出し情報として、暗号化コンテンツ ENCCNT の必ず前側についているとは限らない。例えば、ヘッダ情報 HEAD ではなく、付加情報や検証対象データとして、暗号化コンテンツ ENCCNT の後ろ側（フッタ）についていても構わない。

【0143】

(22) 実施の形態 1 において、コンテンツ CNT が予め n 個に分割されていない場合であっても、暗号化部 105 はある所定の規則に従ってコンテンツ CNT を n 個に分割するようにしても良い。この場合、所定の規則は、例えば、外部から入力されるようにしてもよい。これは、例えば、暗号化部 105 がキーボードやマウスと接続されていることにより実現できる。また、所定の規則は、システム共通のパラメータとして与えられていても良い。ここでのある所定の規則とは、例えば、64 キロバイト単位、1 メガバイト単位、1 秒単位、1 分単位、1 秒単位といった情報である。また、別の例として、コンテンツデータが DVD-VIDEO 形式の動画コンテンツの場合、例えば、VOB 単位や、VOBU (Video Object Unit) 単位、セル (Cell) 単位などである。コンテンツデータが MPEG2 形式の動画コンテンツの場合、例えば、GOP 単位、フィールド単位、フレーム単位、I ピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長 (ECC ブロック単位) などである。なお、それぞれの部分コンテンツの分割単位 (サイズなど) は、全て同じである必要はなく、それぞれ異なっても良い。また、コンテンツを分割する数 (n) は、コンテンツ CNT に応じて変えても良い。また、コンテンツを分割する単位は、また、可搬媒体 11 に記録されているようにしてもよい。

【0144】

(23) 実施の形態 1 において、コンテンツ位置情報 POS は、図 9 のような構成であったが、これに限るものではなく、暗号化部分コンテンツの構成を、及び、暗号化部分コンテンツの中のユニットの構成を特定出来るものであれば、どのようなものでもよい。例えば、特定情報は、暗号化部分コンテンツを識別する光ディスク上の先頭の物理アドレスとデータサイズや、先頭の物理アドレスと終端の物理アドレスであっても良い。さらに、ユニット数の替わりに、各ユニットの先頭の論理アドレスとデータサイズの羅列、もしくは、先頭と終端の論理アドレスの羅列、もしくは、先頭の物理アドレスとデータサイズの羅列、もしくは、先頭と終端の物理アドレスの羅列であっても良い。

【0145】

また、コンテンツ位置情報 POS において、各特定情報に対応する暗号化部分コンテンツに含まれるユニット数が同じ場合、図 30 で示すとおり、 n 個のユニット数の替わりに 1 つの共通ユニット数 ALLNUMU (一つの第二ハッシュ値が、いくつの第一ハッシュ値から計算されているかを示す属性値比率) がコンテンツ位置情報 POS に含まれていても良い。この場合、認証情報 AUTH は、図 31 で示すように、第二ハッシュテーブル H ASHTBL2 及び共通ユニット数 ALLNUMU を連結した値に対する認証情報であっても良く、実行装置 12 における検証時には、認証情報 AUTH が入替第二ハッシュテーブル REPHASHTBL2 及び共通ユニット数 ALLNUMU を連結した値に対する正しい認証情報であるか検証するようにしても良い。

【0146】

(24) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、CD、MO、DVD、SD メモリカード、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とする通信ネットワーク等を経由して伝送するものとしても

よい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記通信ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【0147】

(25) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【0148】

本発明にかかる不正コンテンツ検知システムは、実行装置においてコンテンツを実行開始、もしくは再生開始する前に、そのコンテンツが想定する主体（例えば正規の著作権を有する人・団体・会社）により配布されたコンテンツかどうかを検知できるという機能を有し、その検知結果によりコンテンツの実行開始、再生開始を制御（例えば警告、停止、禁止）することが出来る。これは、コンテンツの著作権保護が必要とされるシステム全般、特に記録媒体や可搬媒体（例えば光ディスクやメモリカード）や通信ネットワーク、放送網を用いたコンテンツ配布システムに有用である。

【0149】

さらに、本発明は、動画データや音声データなどのマルチメディアコンテンツに限らず、コンテンツの実行順序を制御する実行順序ファイル（ナビゲーションファイル）や、コンピュータプログラム等の保護にも適用可能である。この場合、実行装置において、不正なコンピュータプログラム（例えばコンピュータウイルスを含むコンピュータプログラム）を実行開始しない等が実現出来る。そのため、安全（セキュア）な処理環境を実現するコンピュータシステム全般、特にOS（Operation System）等としても有用である。

【図面の簡単な説明】

【0150】

【図1】 本発明の実施の形態1における不正コンテンツ検知システムの概要図

【図2】 本発明の実施の形態1における配布センタ10の構成例を示す図

【図3】 本発明の実施の形態1における実行装置情報格納部103の構成例を示す図

【図4】 本発明の実施の形態1における暗号化鍵束KBの一例を示す図

【図5】 本発明の実施の形態1における暗号化コンテンツENCNTの作成方法の一例を示す図

【図6】 本発明の実施の形態1におけるヘッダ情報HEADの作成方法の一例を示す図

【図7】 本発明の実施の形態1における第一ハッシュテーブルHASH TBL1#1の作成方法の一例を示す図

【図8】 本発明の実施の形態1における第二ハッシュテーブルHASH TBL2の作成方法の一例を示す図

【図9】 本発明の実施の形態1におけるコンテンツ位置情報POSの一例を示す図

【図10】 本発明の実施の形態1における認証情報AUTHの作成方法の一例を示す図

【図11】 本発明の実施の形態1における配布センタ10の処理の流れ図（一例）

【図12】 本発明の実施の形態1における可搬媒体11に記録されるデータの一例を示す図

【図13】 本発明の実施の形態1における実行装置12の構成例を示す図

【図14】 本発明の実施の形態1におけるコンテンツ位置情報POSからi組の特定情報とユニット数を選択する場合の一例を示す図

【図15】 本発明の実施の形態1における入替第二ハッシュテーブルREPHASH TBL2の作成方法の一例を示す図

【図 1 6】本発明の実施の形態 1 における入替第一ハッシュテーブル R E P H A S H T B L 1 # 1 の作成方法の一例を示す図

【図 1 7】本発明の実施の形態 1 における入替第二ハッシュテーブル R E P H A S H T B L 2 の作成方法の一例を示す図

【図 1 8】本発明の実施の形態 1 における認証情報 A U T H の検証方法の一例を示す図

【図 1 9】実行装置 1 2 の処理の一例を示す流れ図

【図 2 0】認証情報生成情報格納部 1 0 7 の別の一例を示す図

【図 2 1】検証情報格納部 1 2 5 の別の一例を示す図

【図 2 2】認証情報生成情報格納部 1 0 7 の別の一例を示す図

【図 2 3】検証情報格納部 1 2 5 の別の一例を示す図

【図 2 4】認証情報 A U T H の別の検証方法の一例（ステップ 1）を示す図

【図 2 5】認証情報 A U T H の別の検証方法の一例（ステップ 2）を示す図

【図 2 6】認証情報 A U T H の別の検証方法の一例（ステップ 2 の詳細 1）を示す図

【図 2 7】認証情報 A U T H の別の検証方法の一例（ステップ 2 の詳細 2）を示す図

【図 2 8】可搬媒体 1 2（光ディスク）と取得部 1 2 1 の一例を示す図

【図 2 9】可搬媒体 1 1 に記録されるデータの別の一例を示す図

【図 3 0】コンテンツ位置情報 P O S の別の一例を示す図

【図 3 1】認証情報 A U T H の作成方法の別の一例を示す図

【図 3 2】認証情報 A U T H の検証方法の別の一例を示す図

【図 3 3】従来技術の可搬媒体に記録されるデータの構成を示す図

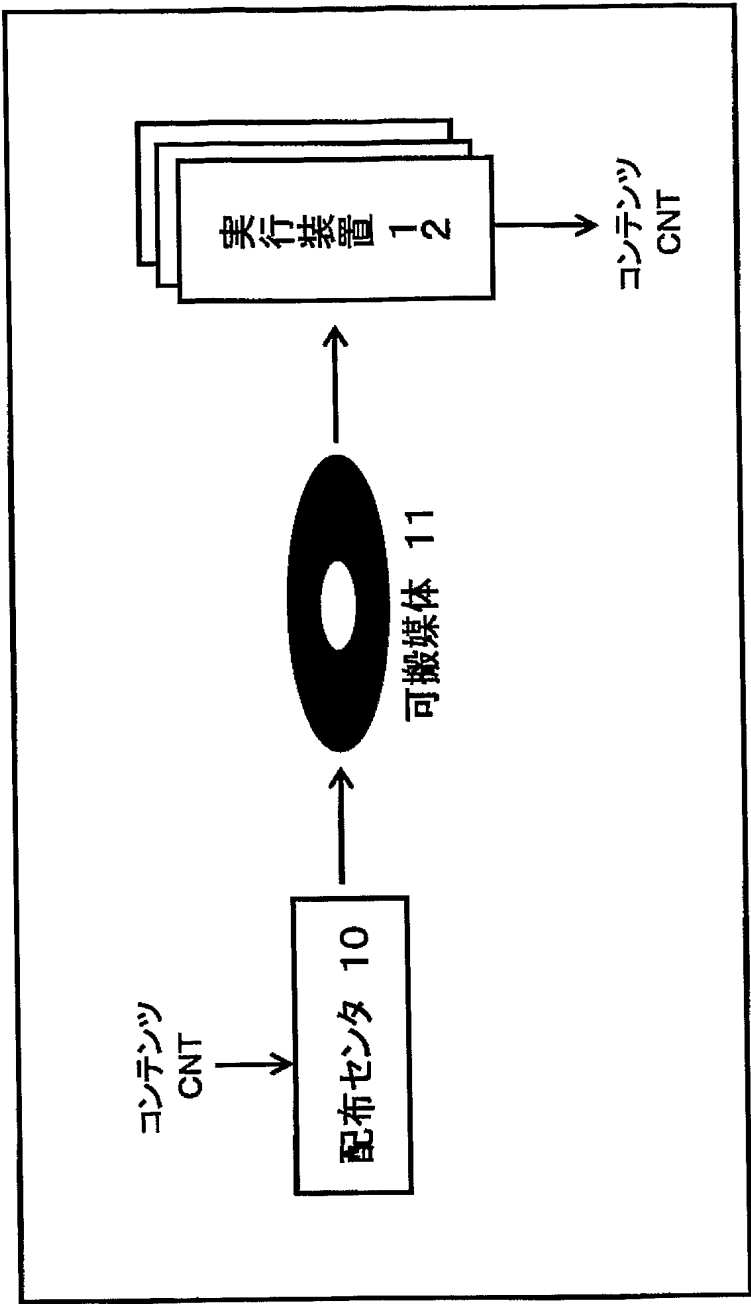
【符号の説明】

【 0 1 5 1 】

1 0	配布センタ
1 1	可搬媒体
1 2	実行装置
1 0 1	入力部
1 0 2	コンテンツ鍵生成部
1 0 3	実行装置情報格納部
1 0 4	暗号化鍵束生成部
1 0 5	暗号化部
1 0 6	ヘッダ情報生成部
1 0 7	認証情報生成情報格納部
1 0 8	認証情報生成部
1 0 9	配布部
1 2 1	取得部
1 2 2	デバイス鍵格納部
1 2 3	コンテンツ鍵取得部
1 2 4	検証情報格納部
1 2 5	認証情報検証部
1 2 6	実行部

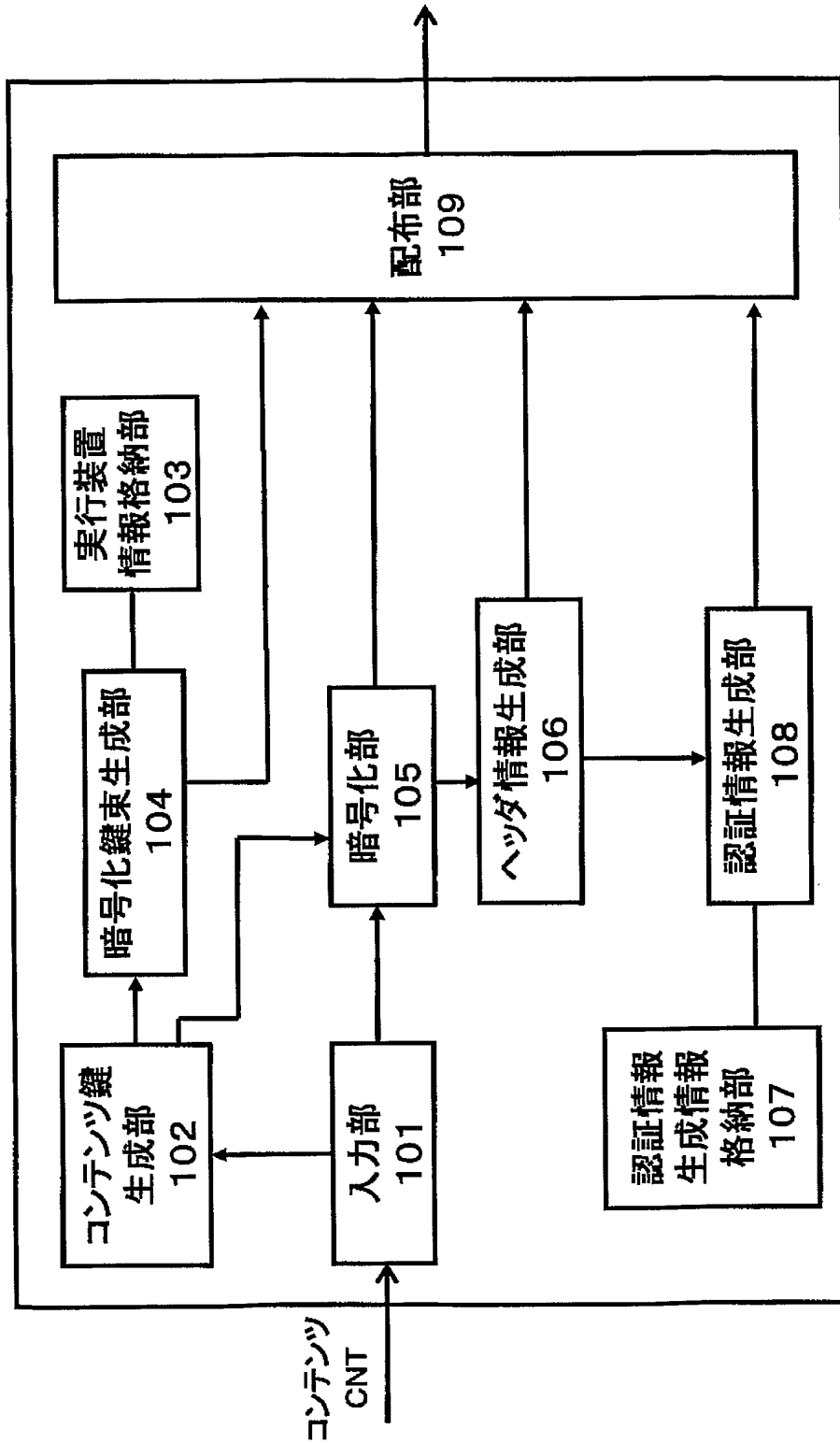
【書類名】 図面
【図 1】

不正コンテンツ検知システム1



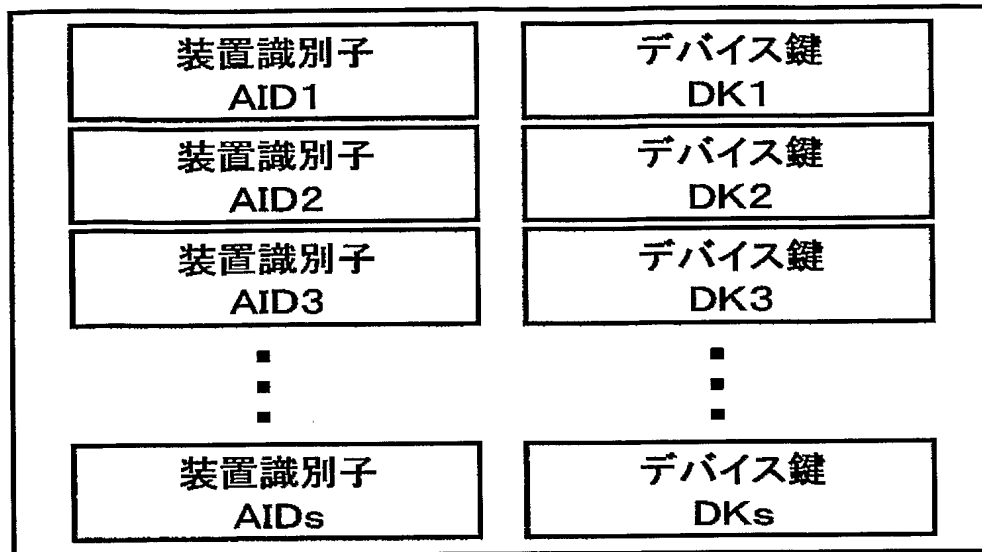
【図 2】

配布センタ 10 の一例



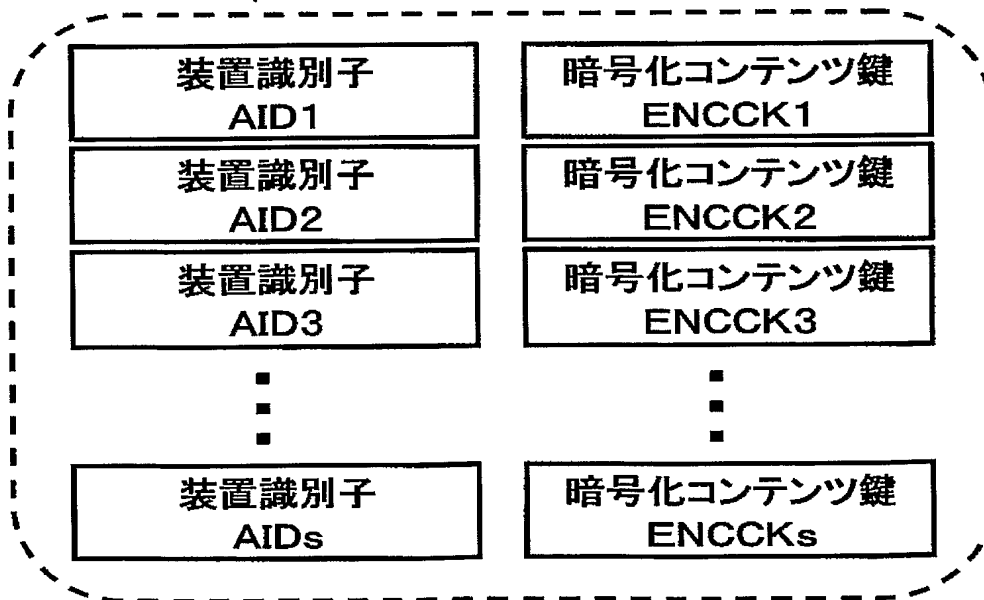
【図 3】

実行装置情報格納部103の一例



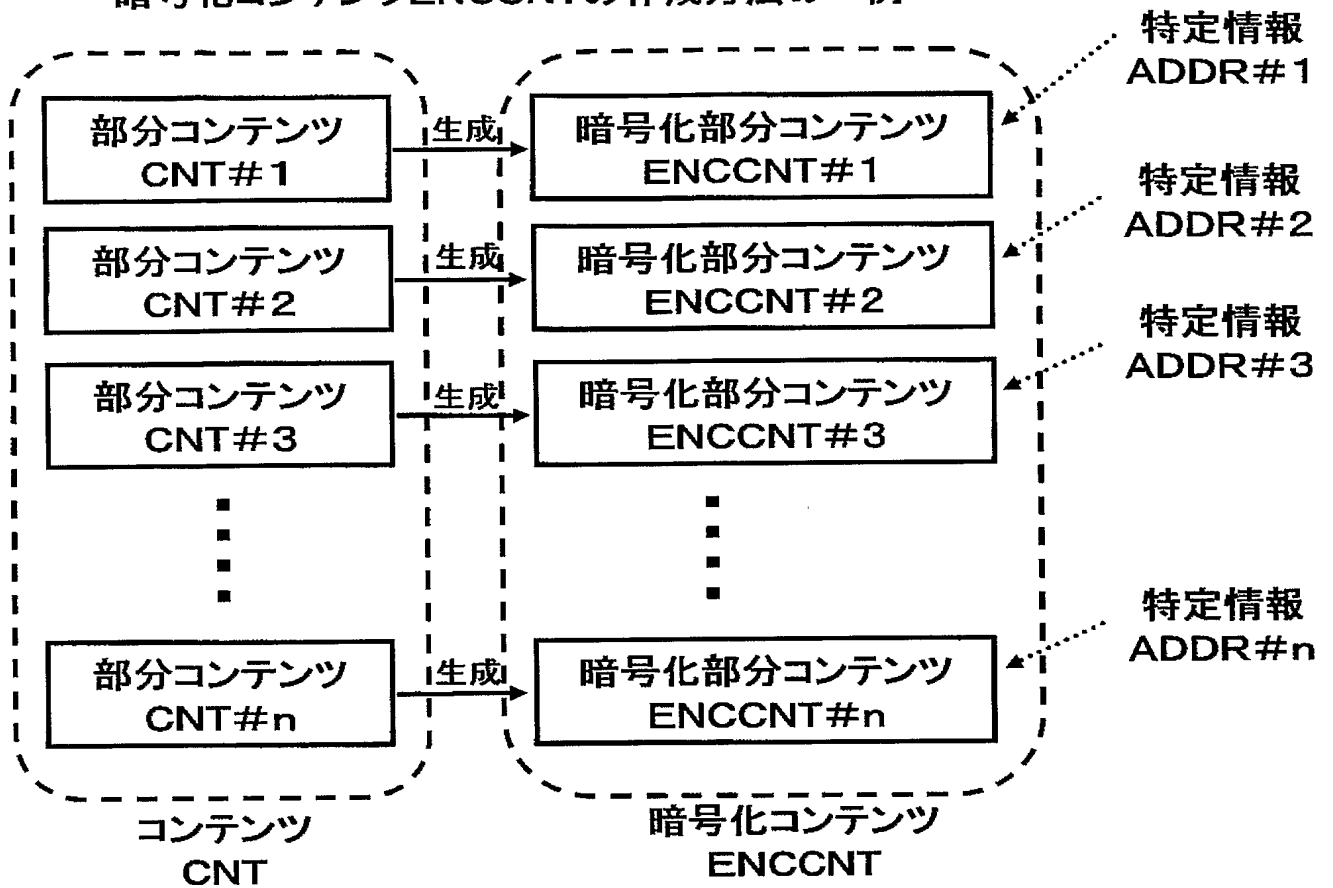
【図 4】

暗号化鍵束 KBの一例



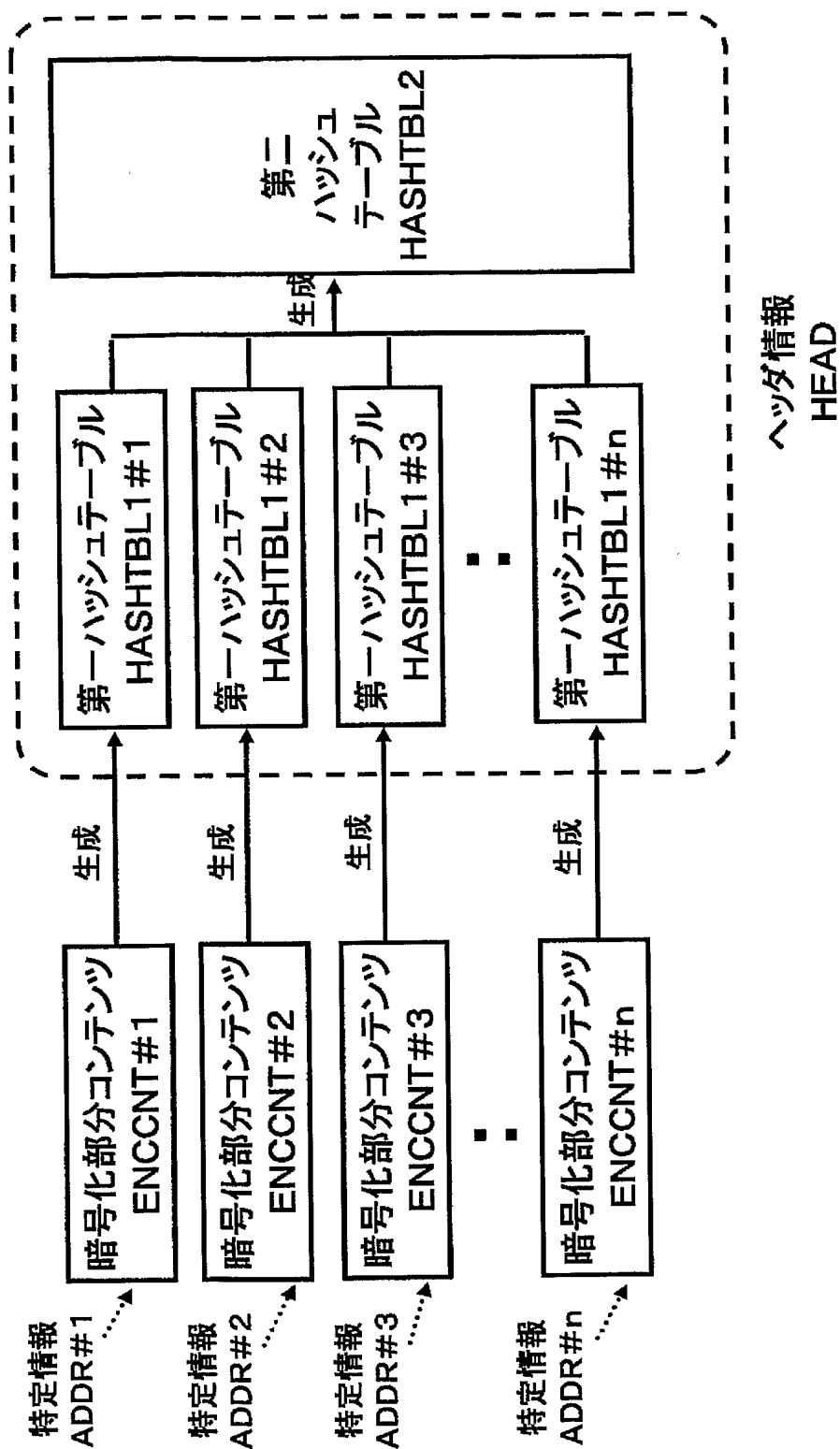
【図 5】

暗号化コンテンツ ENCCNT の作成方法の一例

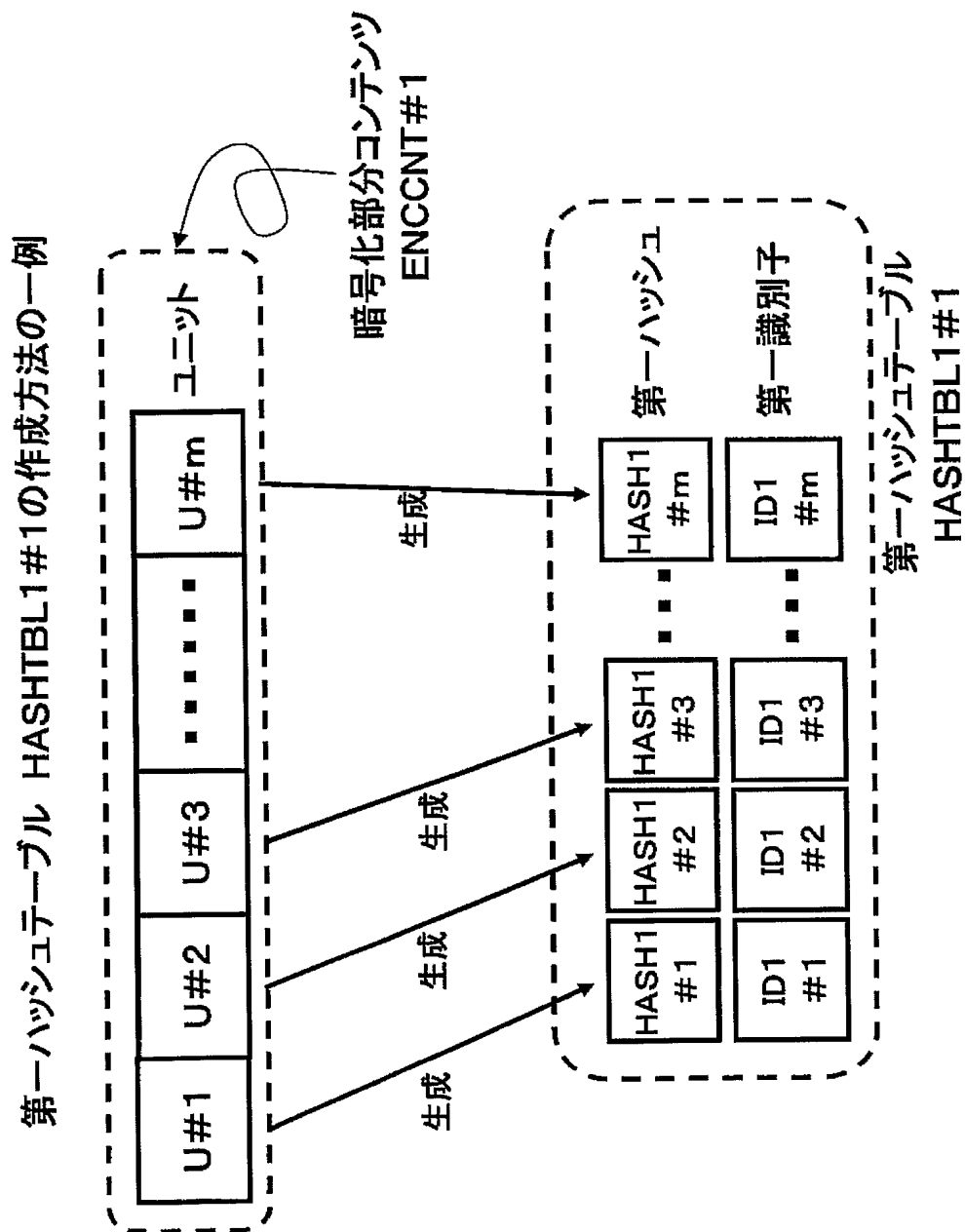


【図 6】

ヘッダ情報HEADの作成方法の一例

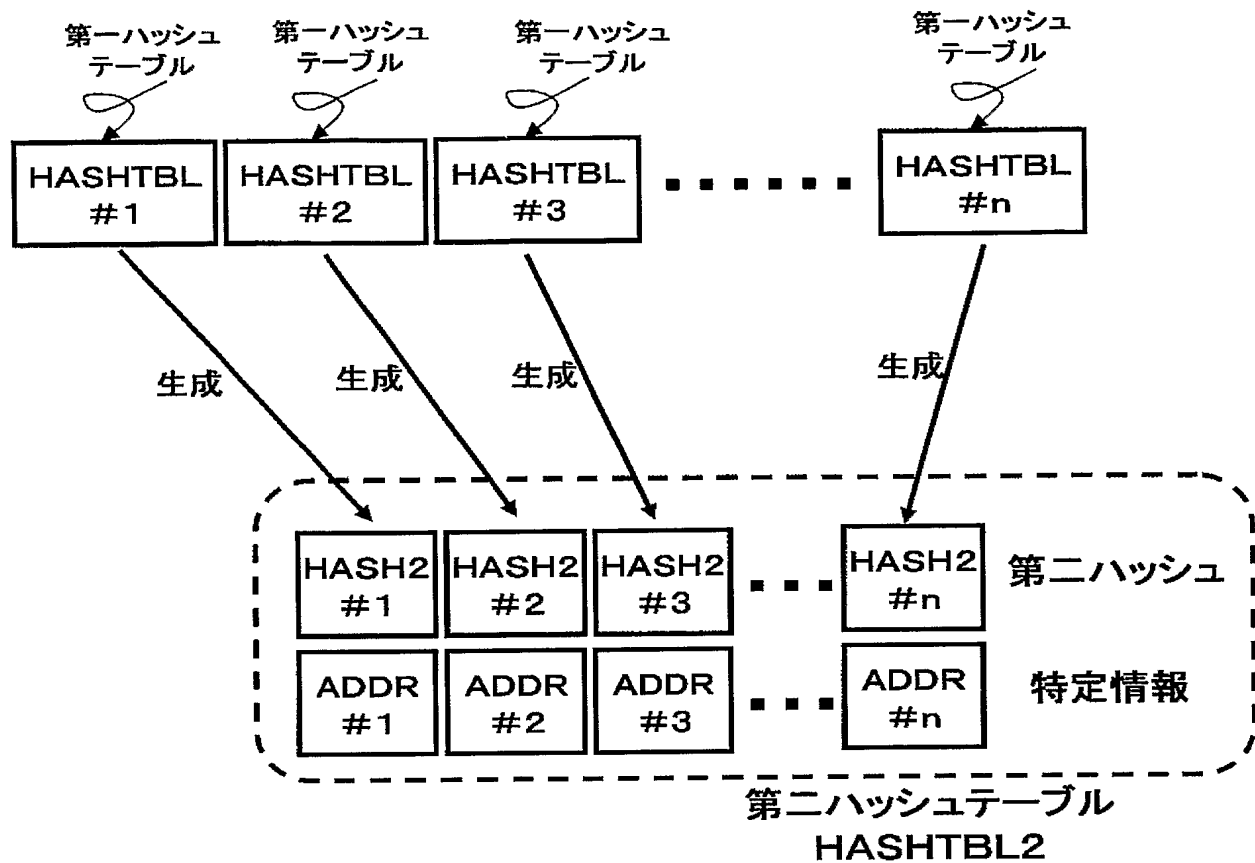


【圖 7】



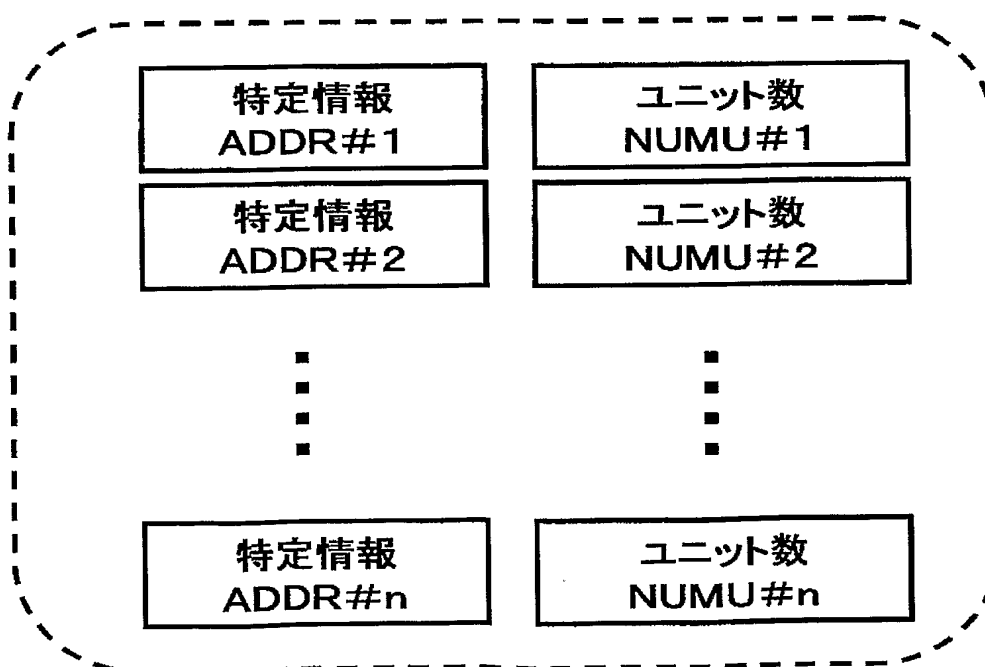
【図 8】

第二ハッシュテーブル HASHTBL2の作成方法の一例



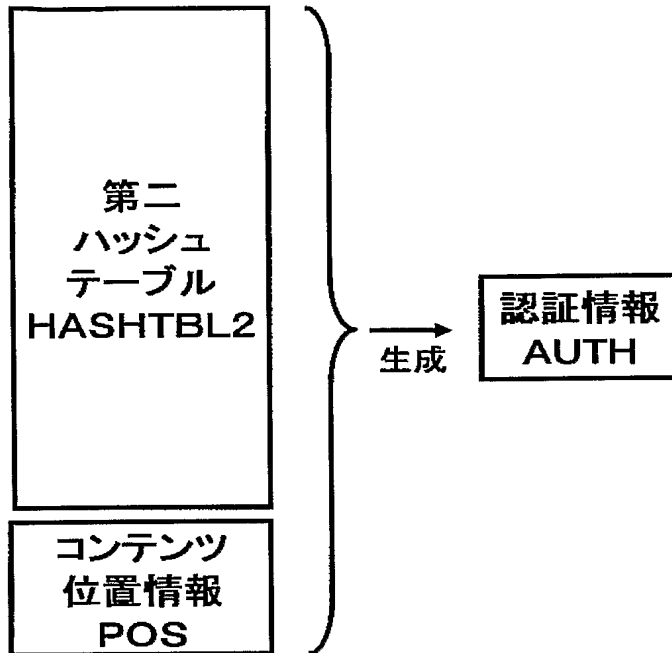
【図 9】

コンテンツ位置情報 POSの一例

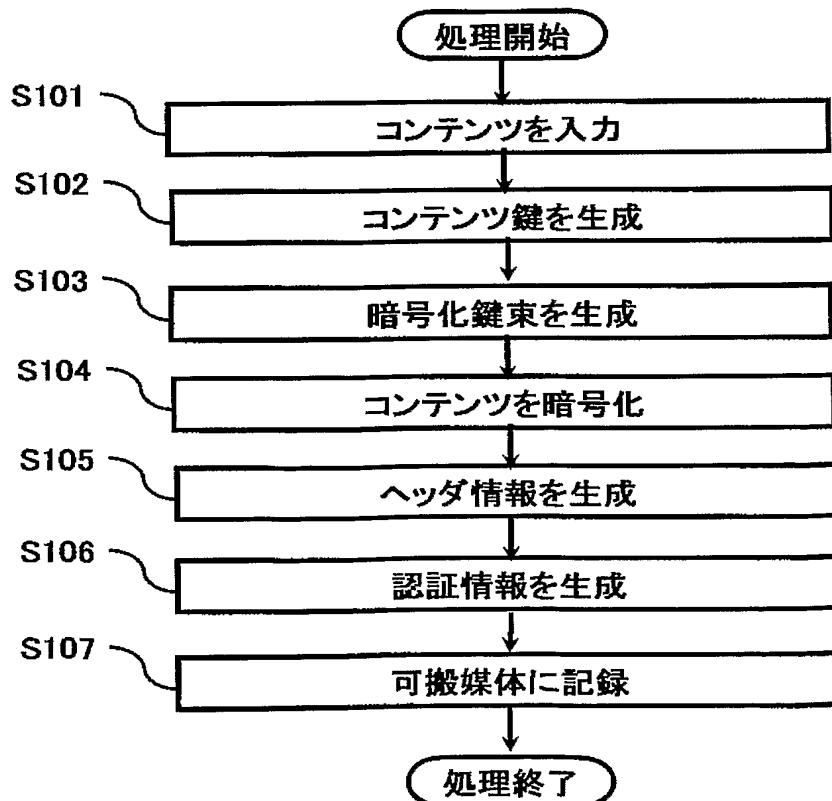


【図 10】

認証情報AUTHの作成方法の一例

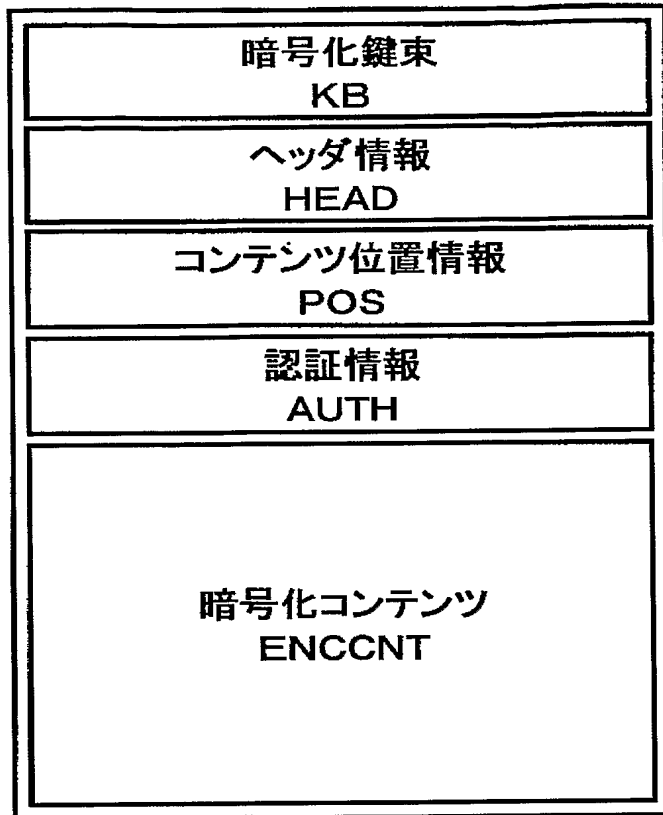


【図 11】



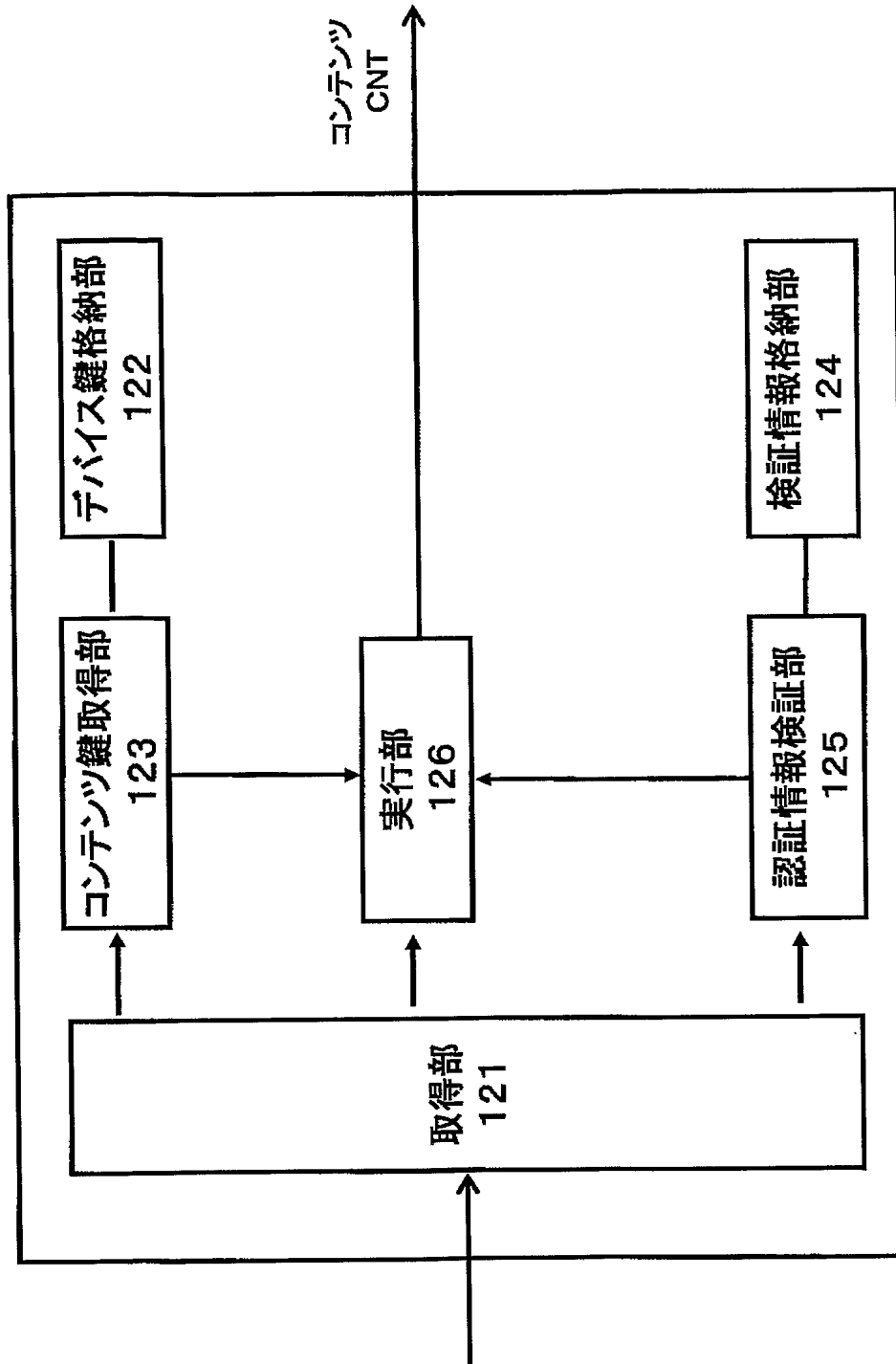
【図 12】

可搬媒体 11 に記録されるデータの一例

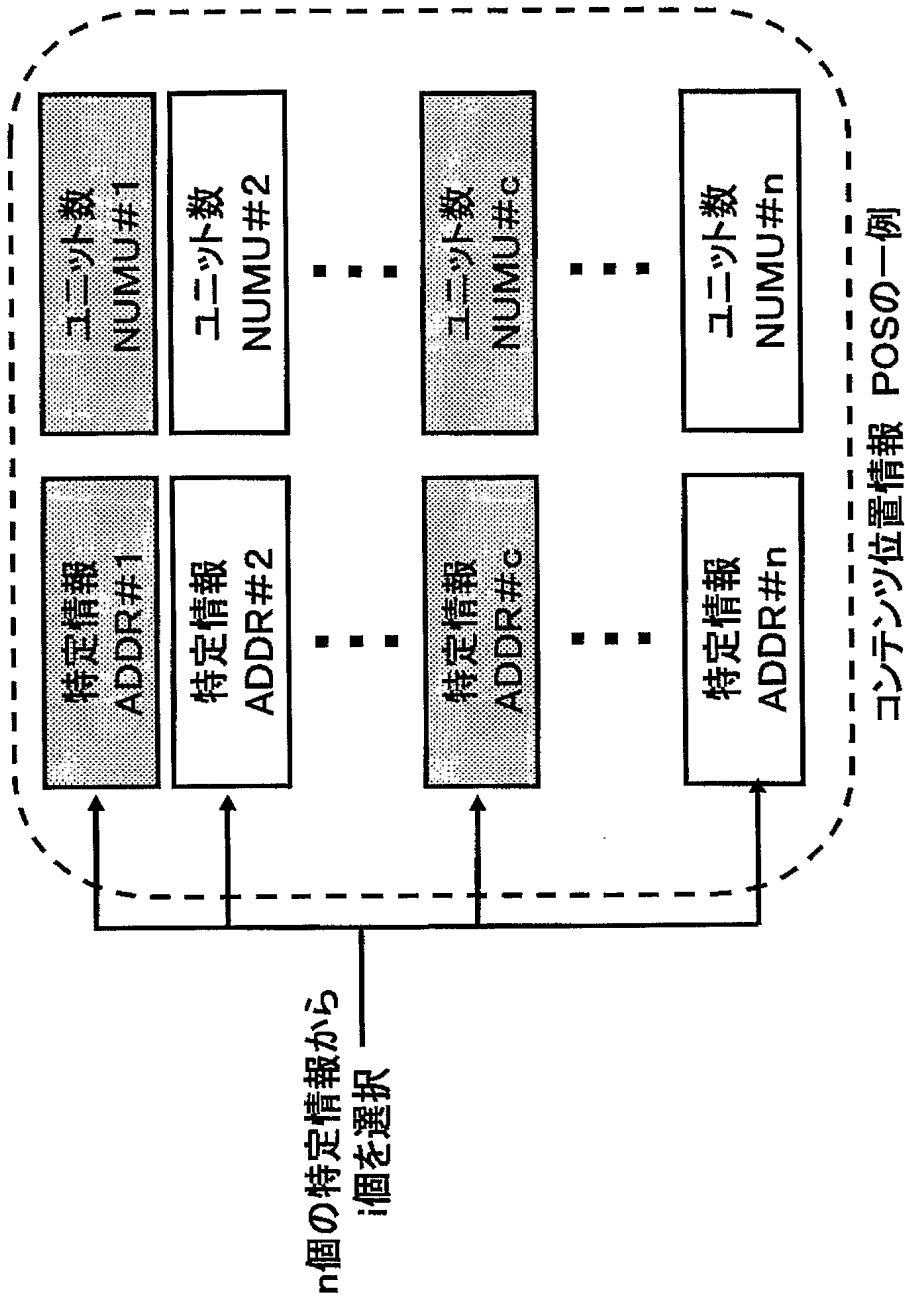


【図 13】

実行装置 12 の一例

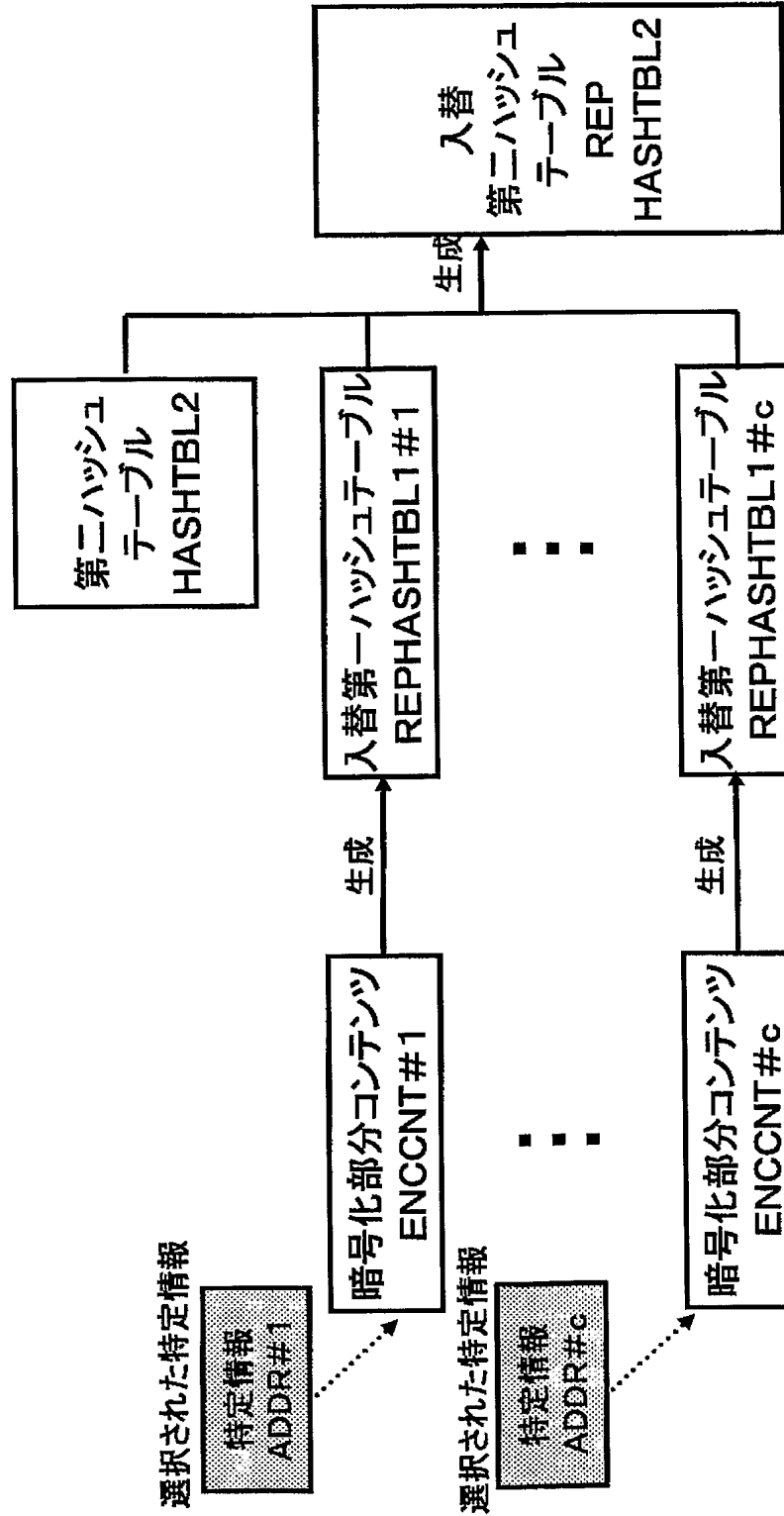


【図 14】

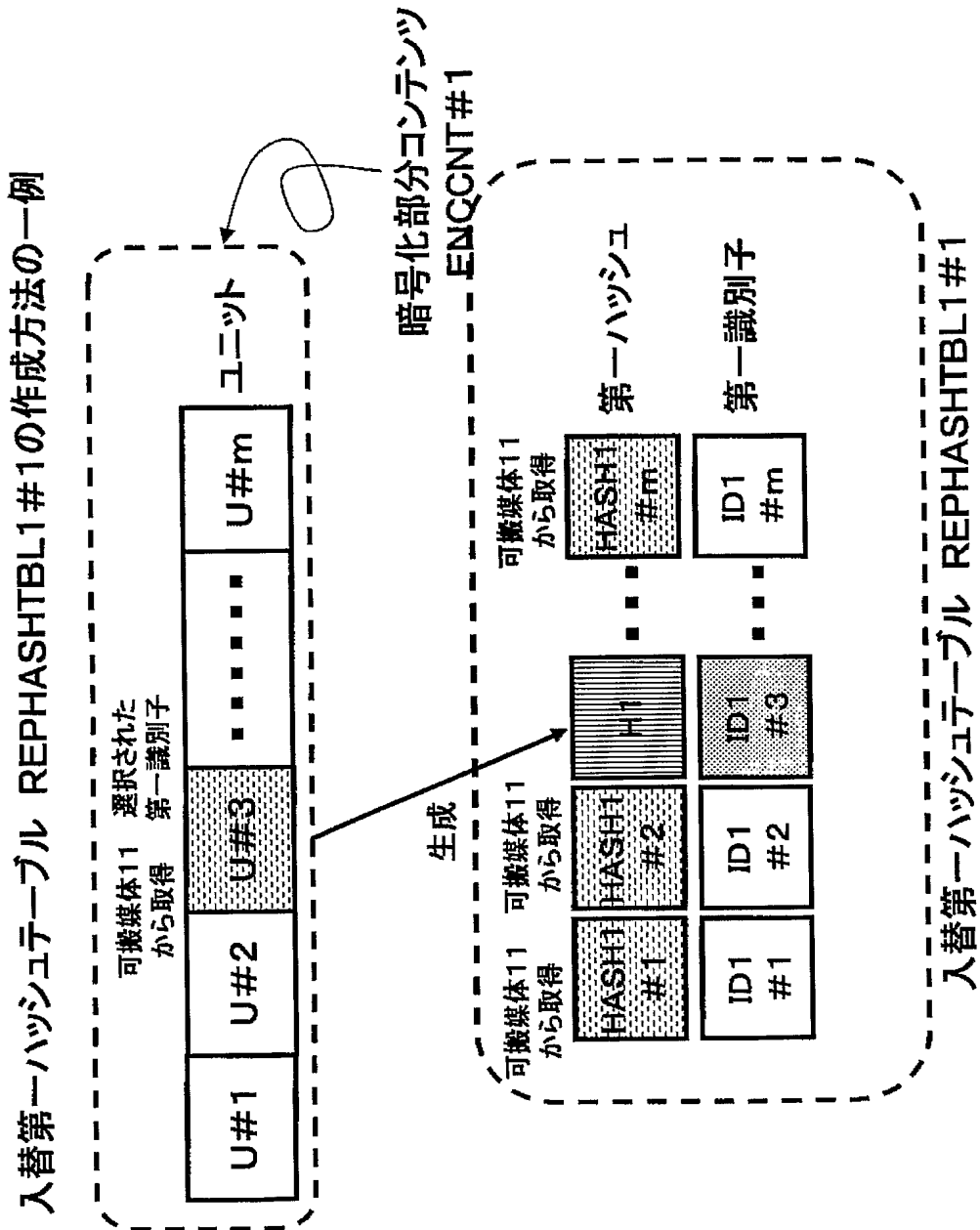


【図 15】

入替第二ハッシュテーブルREPHASHTBL2の作成方法の一例

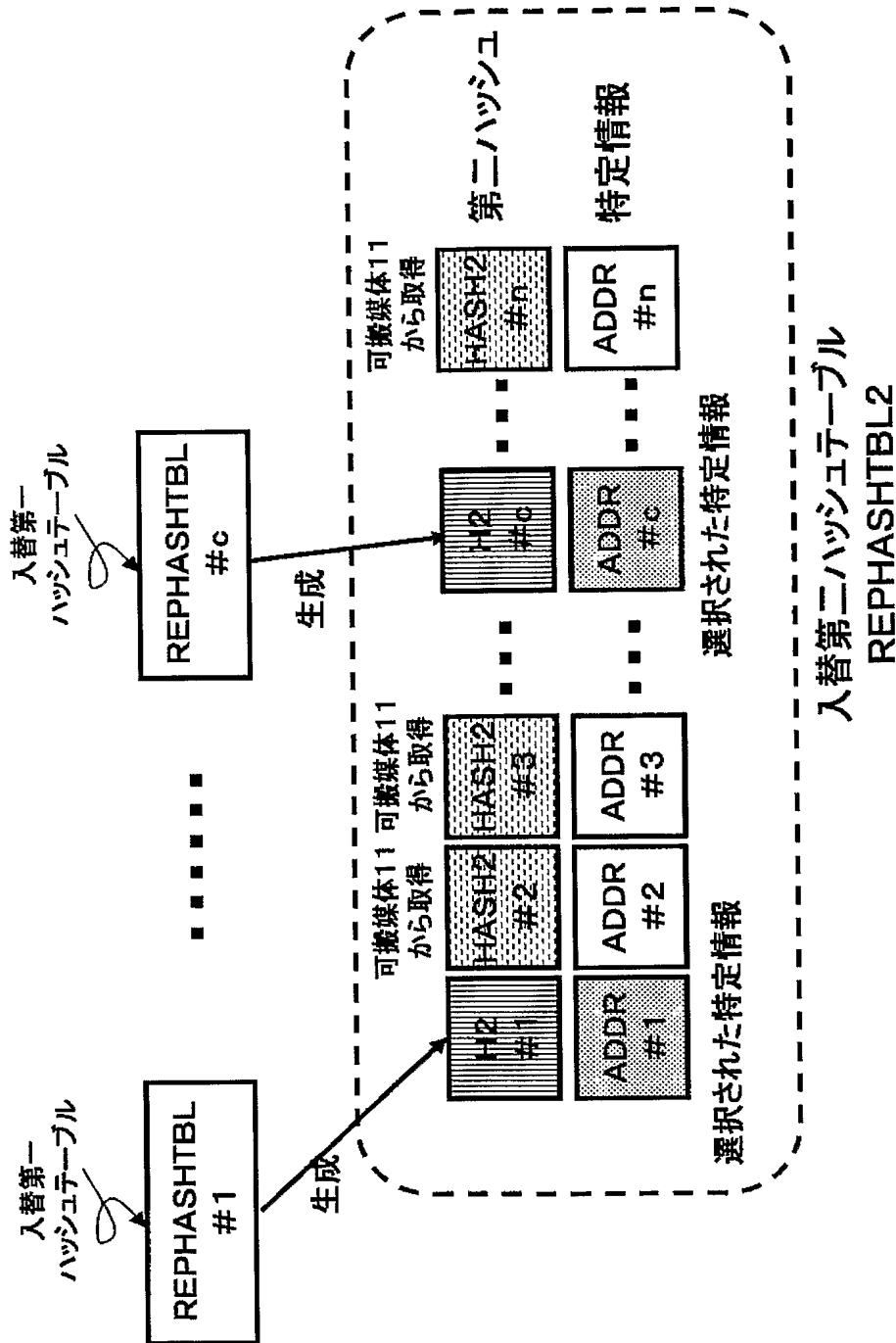


【図 16】



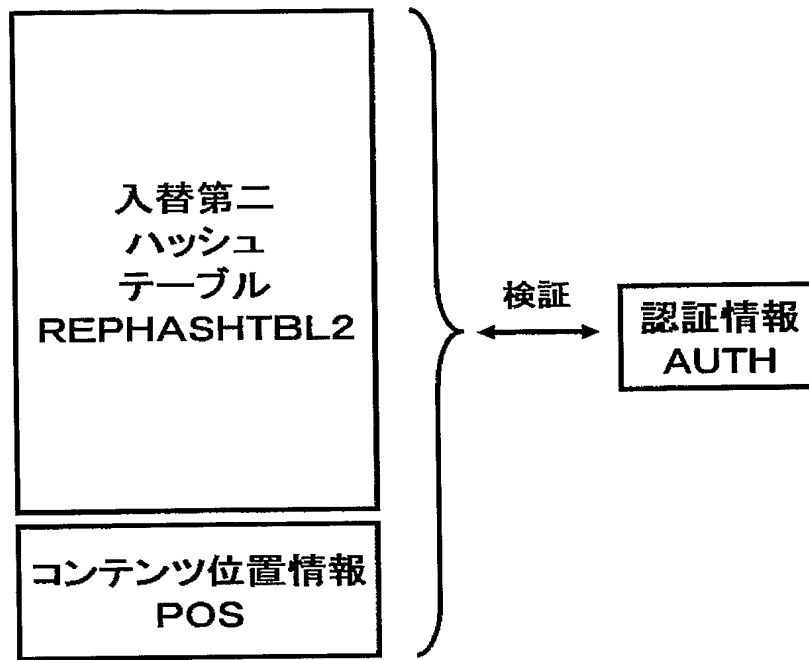
【図 17】

入替第二ハッシュテーブル REPHASHTBL2の作成方法の一例

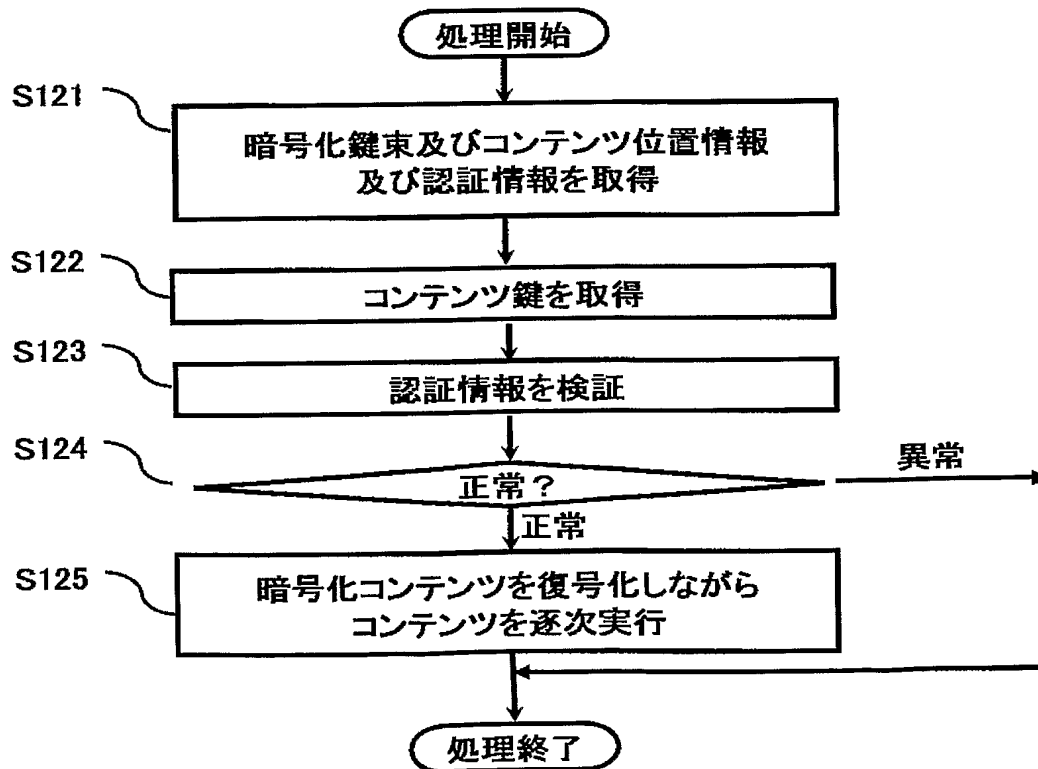


【図 18】

認証情報AUTHの検証方法の一例

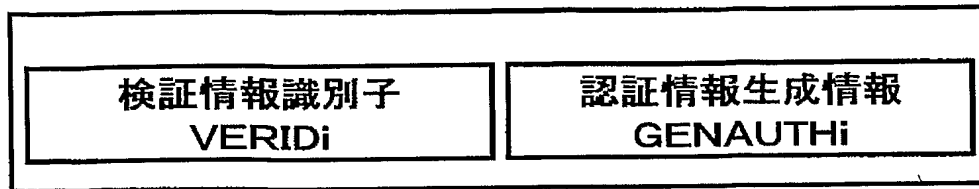


【図 19】



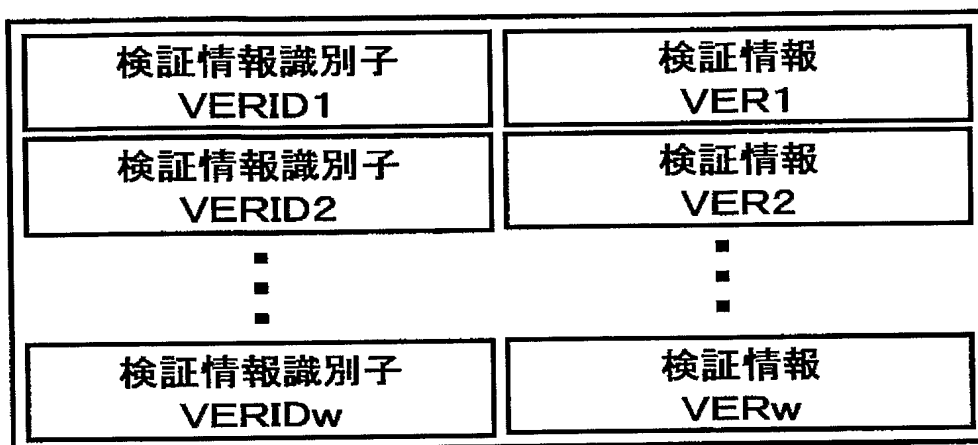
【図 20】

認証情報生成情報格納部107の別の一例



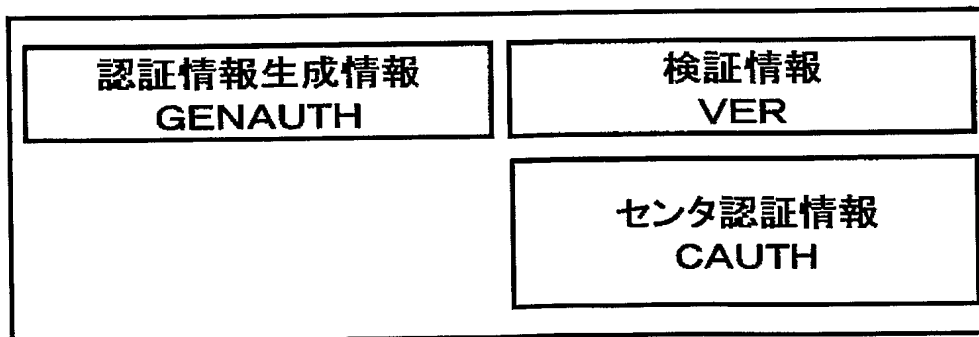
【図 21】

検証情報格納部125の別の一例



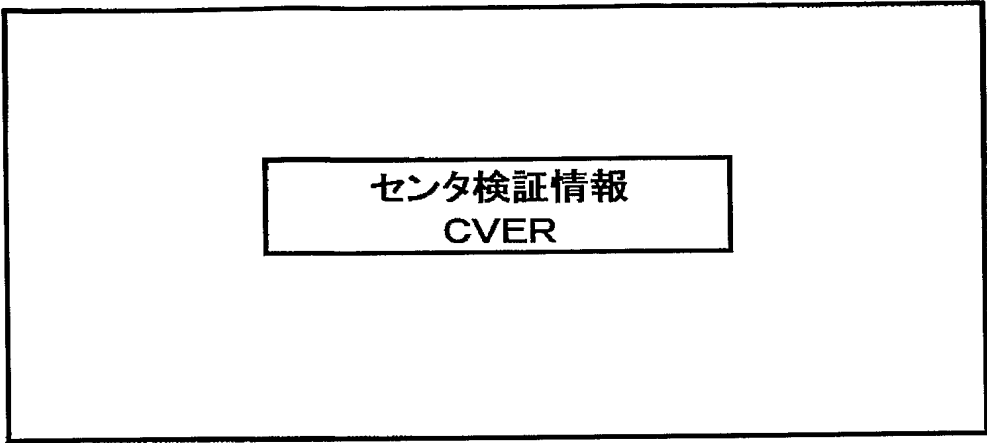
【図 22】

認証情報生成情報格納部107の別の一例



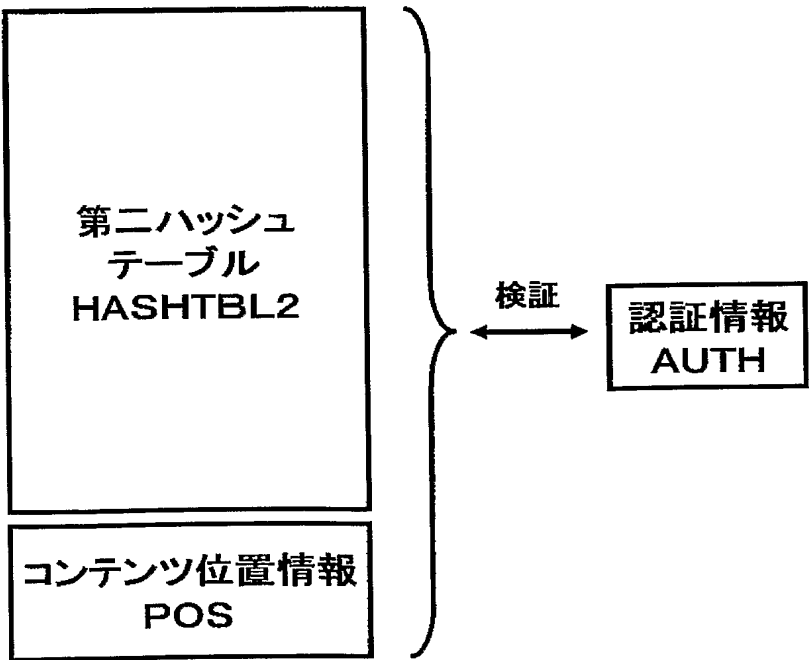
【図 2 3】

検証情報格納部125の別の一例



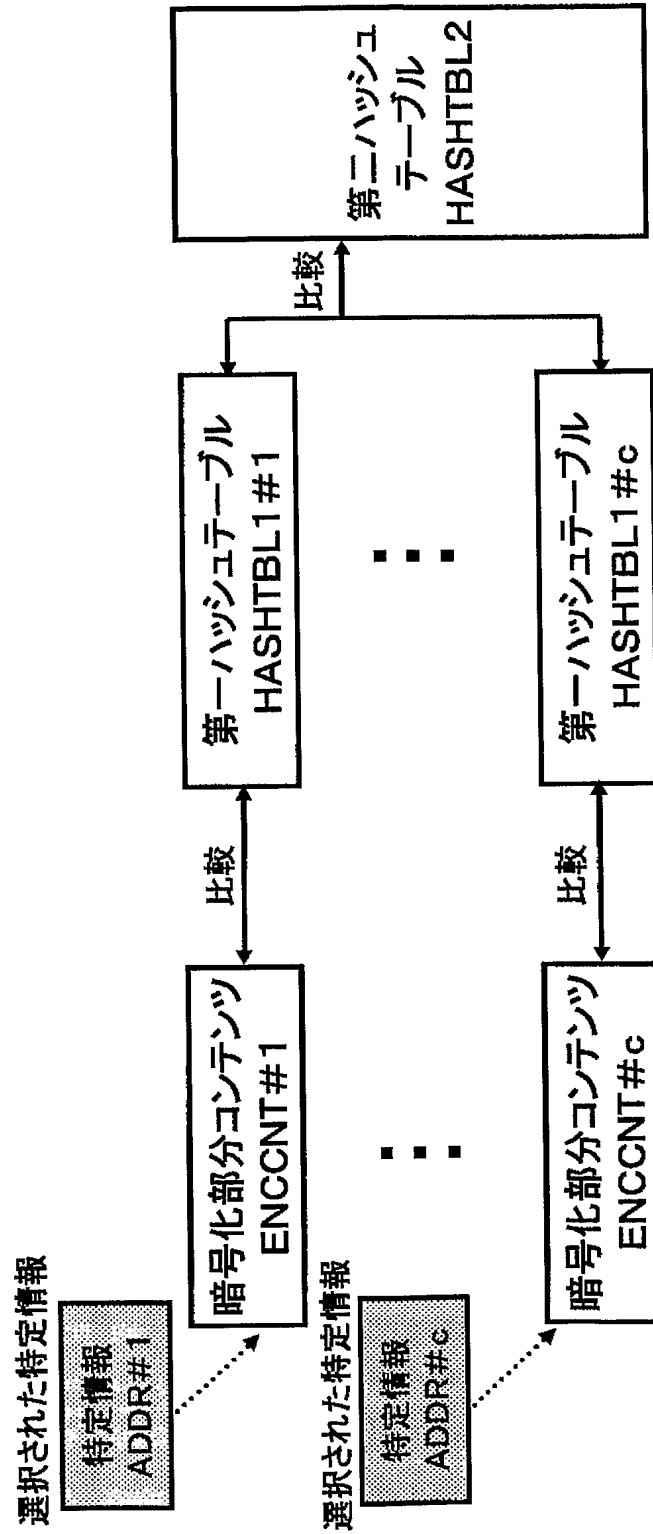
【図 2 4】

認証情報AUTHの別の検証例(ステップ1)



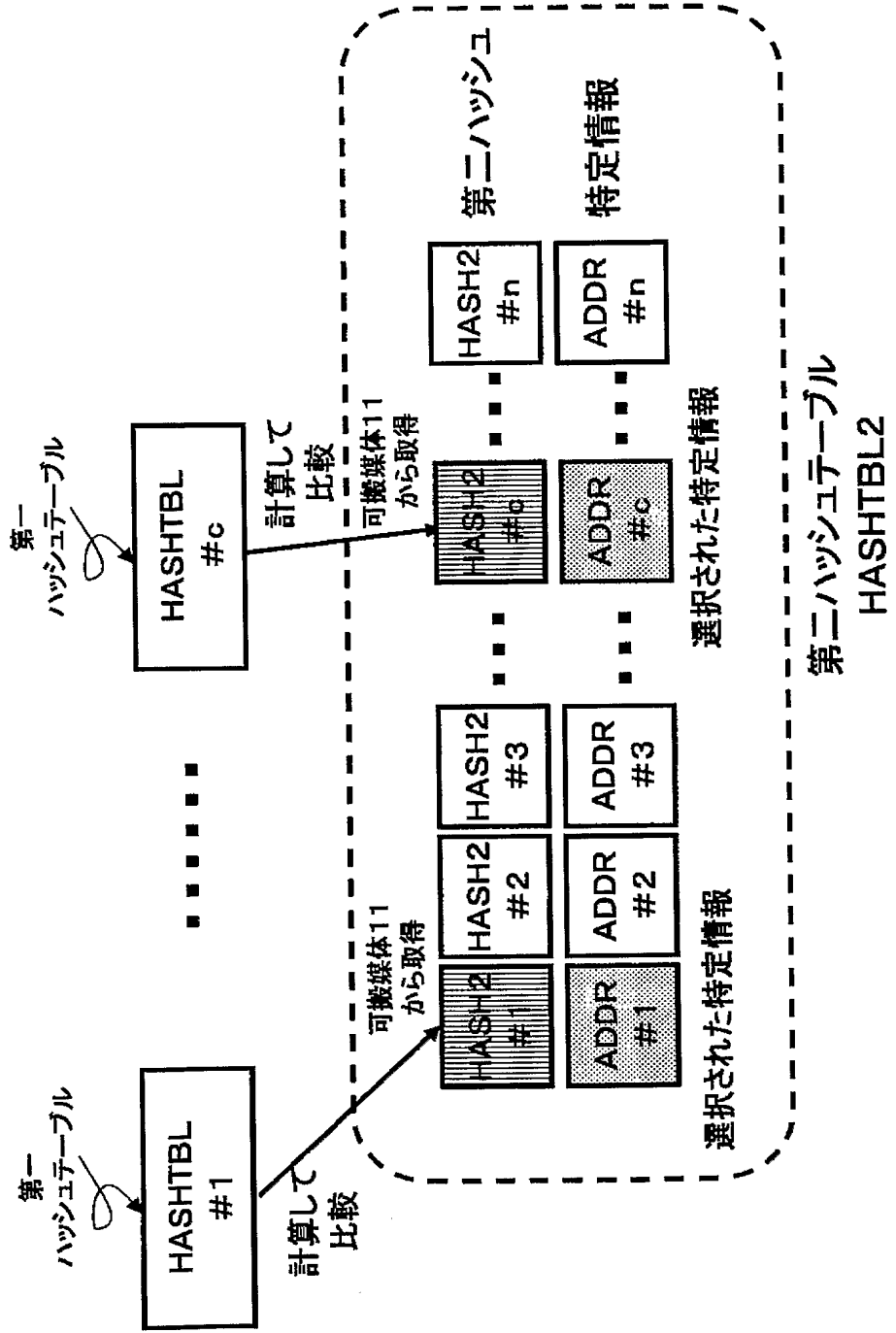
【図 25】

認証情報AUTHの別の検証例(ステップ2)

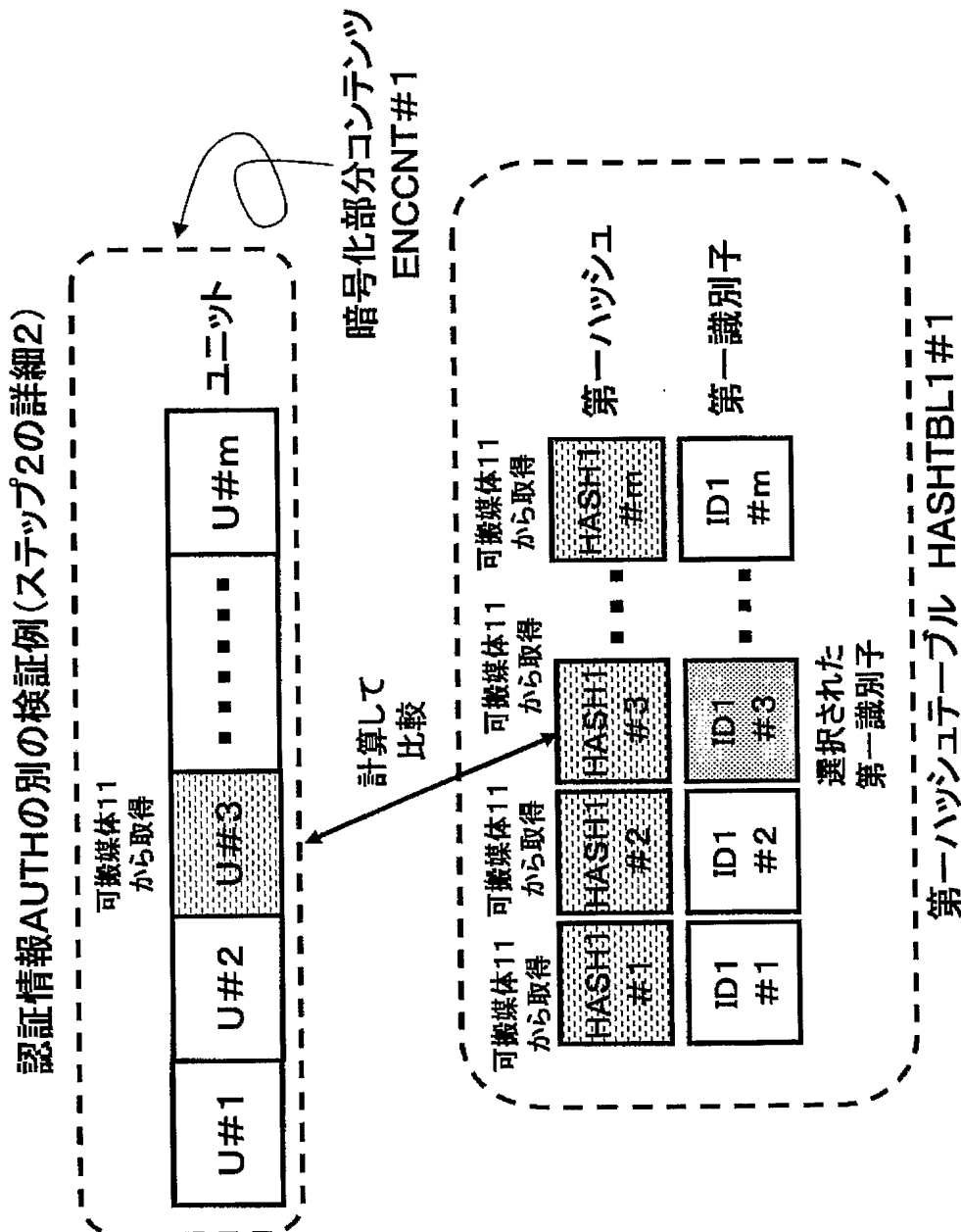


【図 26】

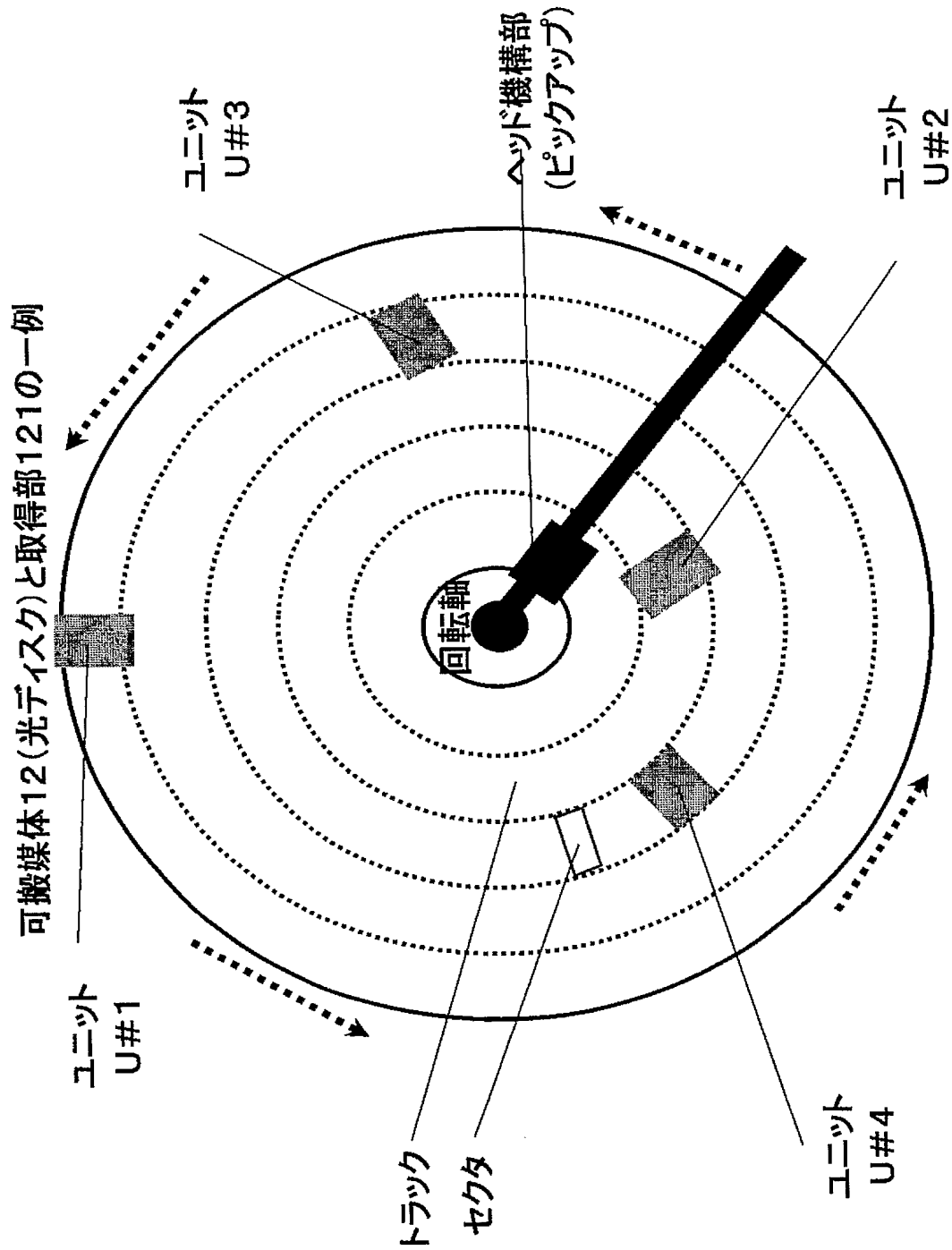
認証情報AUTHの別の検証例(ステップ2の詳細1)



【図 27】

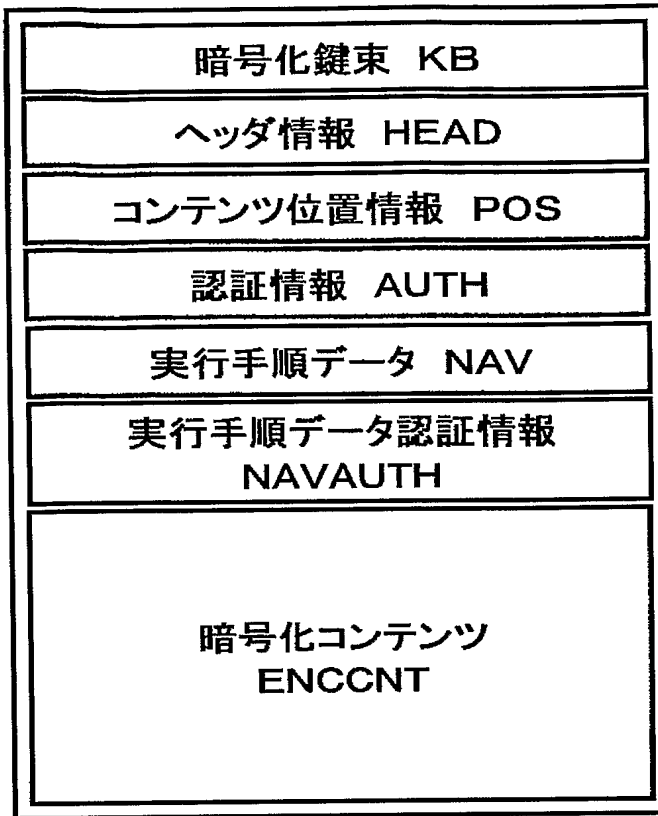


【図 28】



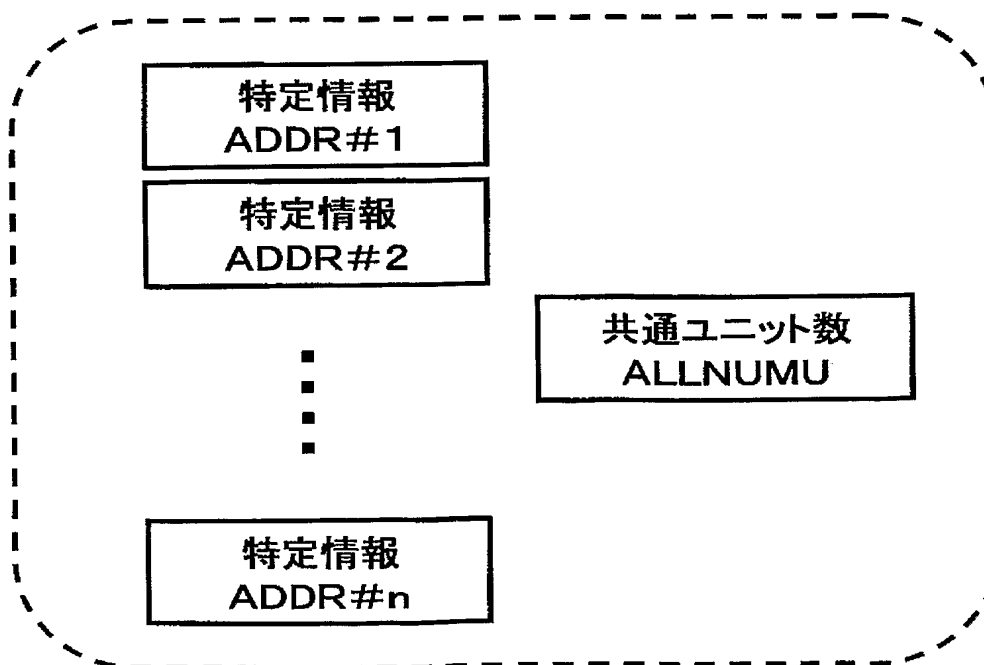
【図 29】

可搬媒体11に記録されるデータの別の一例



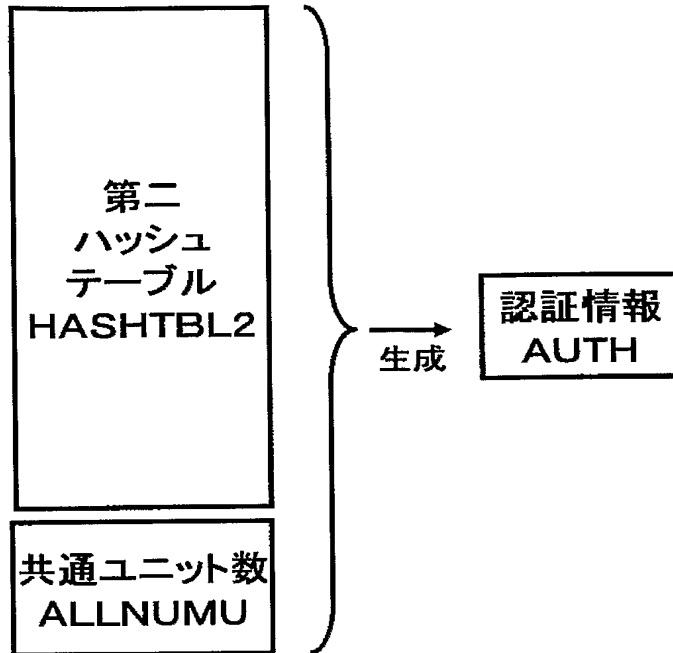
【図 30】

コンテンツ位置情報 POSの別の一例



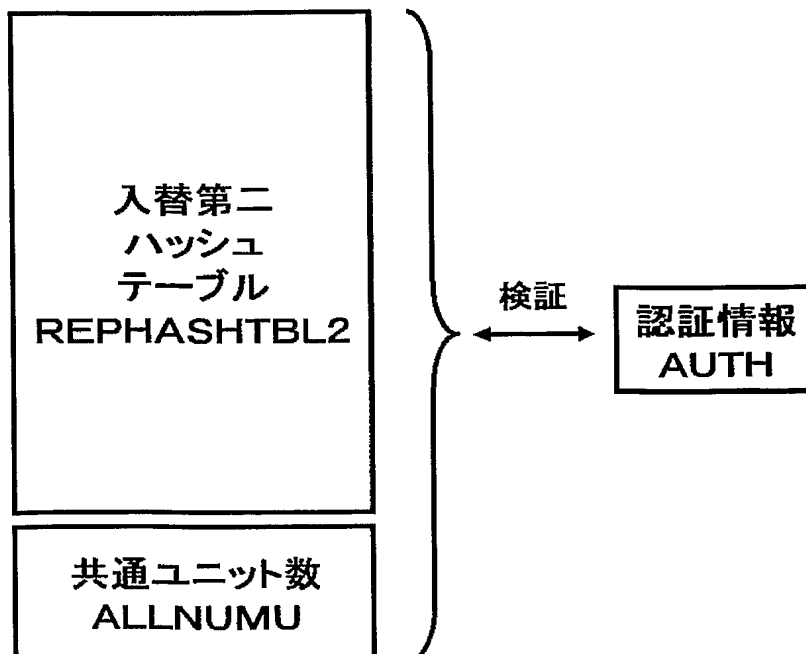
【図 3 1】

認証情報AUTHの作成方法の別の一例



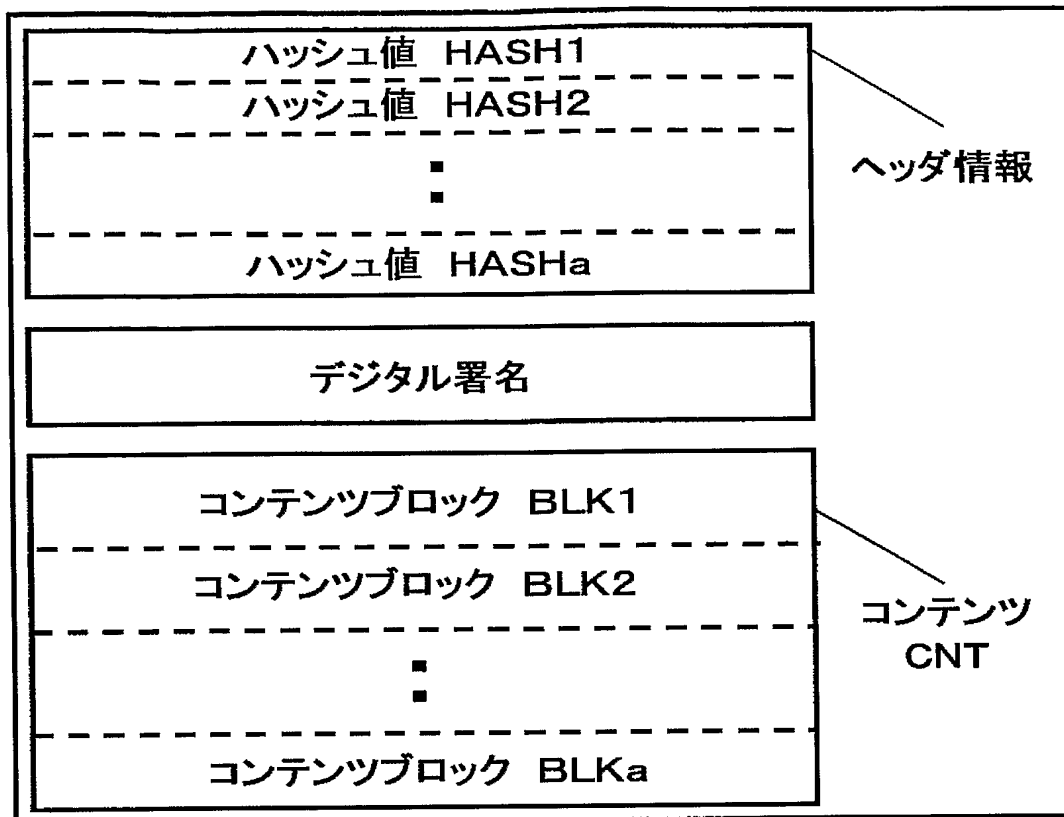
【図 3 2】

認証情報AUTHの検証方法の別の一例



【図 33】

従来技術の可搬媒体に記録されるデータ



【書類名】要約書

【要約】

【課題】 実行装置において不正コンテンツかどうか検知する処理において、コンテンツ実行中の処理負荷が大きかった。

【解決手段】 配布センタ 10 が、暗号化されたコンテンツ CNT とともに、ヘッダ情報 HEAD、及び、コンテンツ位置情報 POS、及び、認証情報 AUTH（例えばデジタル署名）を可搬媒体 11 に記録し、実行装置 12 では、コンテンツ CNT の実行、再生開始前に、認証情報 AUTH が正規の認証情報（例えばデジタル署名）であるか検証する際に、コンテンツ位置情報 POS に含まれる n 組の特定情報 ADDR#1、・・・、ADDR#n とユニット数 U#1、・・・、U#n から、i 組の特定情報とユニット数を選択し、一部のハッシュ値に絞って検証することにより、コンテンツ CNT を実行、再生開始する毎に、異なるハッシュ値を選択する。

【選択図】 図 1

特願 2 0 0 4 - 1 9 6 5 3 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社